2

SCIENCE APPLICATIONS, INC.

2

COUNTERING TERRORISM ON MILITARY INSTALLATIONS

FINAL REPORT

ATLANTA • ANN ARBOR • BOSTON • CHICAGO • CLEVELAND • DENVER • HUNTSVILLE • LA JOLLA
LITTLE ROCK • LOS ANGELES • SAN FRANCISCO • SANTA BARBARA • TUSCON • WASHINGTON

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) (6) Countering Terrorism on Military Installations.	(9)	5. TYPE OF REPORT & PERIOD COVERED Final rept. 31 Aug 76 - 1 Aug 77
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) (10) Mr. Roland B./Shriver, Jr., Mr. John C./Evans Mr. Marvin/Leibstone	(15)	8. CONTRACT OR GRANT NUMBER(s) MDA903-76-C-0272
9. PERFORMING ORGANIZATION NAME AND ADDRESS Science Applications, Inc. 8400 Westpark Drive McLean Virginia 22101		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS HQ, Department of the Army DAPE-HRE Washington, DC 20310	(11)	12. REPORT DATE 29 July 1977
		13. NUMBER OF PAGES 276
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office) Same as Item 11	(12) 221p.	15. SECURITY CLASS. (of this report) UNCLASSIFIED
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

Same as item 16

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

International, Transnational and Domestic Terrorism; Threat Analysis; Crisis Management; Awareness Training; Targets; Intelligence; Field Operations/Combative Organization/Tactics, Installation Vulnerability; Intelligence Problem; Terrorist Incidents; Threat Perception in CONUS

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This study Study examines the implications that threats of terrorism have for current and future missions of the Army. It determines the future role of the military police in countering terrorist acts. It recommends revision required in the Army's law enforcement doctrine, structure, training, equipment and planning to counter acts of terrorism when they occur. The authors ~~study~~ examine ~~s~~ ~~and makes recommendations~~ the question whether the Army should adopt broad policy guidance or specified guidance to subordinate commands in dealing with acts of terrorism. They It examine ~~s~~ the Army's and make recommendations [illegible]

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

408 404

UNCLASSIFIED LB

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

20. (cont)

capability to thwart criminal/terrorist efforts at sabotage, blackmail, or other disruptions on US Army installations worldwide. The study recommends appropriate countermeasures, including education and awareness training ~~which~~ should be implemented at installation level both in and OCONUS.

COUNTERING TERRORISM
ON
MILITARY INSTALLATIONS

Final Report

Rowland B. Shriver, Jr.
John C. Evans.
Marvin Leibstone

Submitted to:
Department of the Army
DCSPER-HRE-PO

In Compliance with Contract No:
MDA903-76-C-0272

29 July 1977

SCIENCE APPLICATIONS, INC.
8400 Westpark Drive
McLean, Virginia 22101

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

The authors wish to express their appreciation to the many individuals and organizations who gave of their time, effort, advice and encouragement which enabled this work to be performed.

In particular we are grateful to Deputy Chief Richard Rabe, Washington, D. C. Metropolitan Police for his valuable comments and Major James Needham, Ft. Leavenworth, Kansas for his contribution in the area of Hostage situations.

The SAI study team was fortunate to have as the contracting officer's technical representative a dedicated career professional, LTC Donald M. Gallagher. The close working relationship that was established at the outset of this study contributed significantly to this final report. We were also very fortunate to have available people who managed to translate our writing into a readable form, especially Pam Hagel and Pam Girlando.

I. INTRODUCTION

Although political terrorism has captured headlines for almost a decade, its main blows have spared the United States. The civil disturbance events of the 1960s in America are pale alongside the violence and sensationalism of European and Palestinian terror. However, with modern transportation, modern arms, and a rising demand for public attention, the reach of political terror is global. Future terror could be directed against stronger, better defended American targets, including Army installations. Total protection from terrorists is impossible; however, Science Applications, Inc. dedicated itself to finding the most practical and economical means to thwart terrorism on U.S. Army installations. This study provides ways for the Department of the Army to upgrade policy and directives which will provide commanders and staffs at all levels with methods designed to deter terrorism, and if it occurs, to minimize its impacts on personnel and other resources vital to the Army's missions. The value of this study will not be in developing new knowledge, insights, or exotic formulae - its real worth must be measured in helping to make practical decisions on allocation of limited resources to protect Army installations against terrorism. Money and people are in limited supply. Manpower and money costs may be minimized by judicious changes in policy, procedures, training and indoctrination. The SAI study team consistently sought to optimize use of existing resources before invoking needs to commit additional resources.

The first months of this study concentrated on collection, collation, and analysis of threat documentation, policy papers, directives, field trips CONUS and OCONUS, and preparation of a comprehensive threat analysis. This was followed by a period of not only continued in-depth research but evaluations and probability matchings of concepts for the development of countermeasures. Two surveys were completed in order to lend credence to emerging concepts, and visits to subject matter experts were made to round out theory and practical methods. These included intelligence agencies and metropolitan police officials.

II. THE STUDY APPROACH

To prevent gaps in the study, and to prioritize study components, the SAI study team designed a detailed matrix to provide a structured analysis of the various aspects of countering terrorism on military (Army) installations. This was necessary in order to develop a better understanding of terrorism and development or appropriate countermeasures. Five basic analysis task categories were established, these being:

- Crisis Management
- Awareness (Education and Training)
- U.S. Army Capabilities (Personnel and Equipment)
- Targets
- Intelligence.

These categories received analysis in three distinct orientations or phases: pre-event, event, and post-event. It was recognized early in the study that actions required for each phase were different prior to terroristic acts, during, and subsequent to the act.

III. THREAT ANALYSIS

SAI prepared an analysis of terrorist developments and actions focusing on information useful to understandings of possible future terror against the U.S. Army. Provided with this report, at Appendix A is the analysis titled, "International, Transnational and Domestic Terror: A Threat Analysis". This document includes significant facts and key judgements, examples of which follow:

- There are more than 140 terrorist organizations operating in 50 countries, at least 13 of which are in the United States. Since 1968, these organizations have conducted more than 900 operations, taking 800 lives and wounding 1,700. Of total incidents, more than 300 involved US citizens or property as direct victims or targets.

Between 1968 and 1975, there were more than 100 terrorist acts against DOD personnel and targets . . . in 1975, of 28 acts against DOD, 9 involved US Army targets.

- Among terrorist organizations OCONUS are the Baader-Meinhof Gang (FRG), the Japanese Red Army, the PLO Al-Fatah, the PFLP, Black September, and the "Carlos" Group (transregional).
- Terror will probably continue at around 200 incidents annually, with 20-30 incidents against DOD installations.
- Transnational terror - that by groups NOT governed by sovereign states - will continue to pose the more serious threat.
- Terrorists will seize nuclear facilities more to obtain demands than steal or activate weapons.
- Terrorist operational tactics will remain swift and violent by trained personnel.

The actions of terrorist groups and their stated objectives imply the US Army will continue to be confronted with terrorist incidents. More probable are acts by individual terrorists, individual domestic and transnational groups, and by cooperating domestic and transnational groups. Less probable are acts by groups developed for warfare by nations whose interests are in conflict with those of the United States. To counter either, the US Army will need policies and plans to maximize resources for appropriate intelligence, and tactical operations.

Inter-dis.iplinary crisis-management techniques will be required at command and field operational levels, and US Army law-enforcement and other designated counter-terror forces will need to develop prec.se tactical applications for terrorist situations in-progress, to include specific rules of engagement and negotiating/bargaining methods. Potential terrorist targets will have to be identified and qualified . . . These comments are not new. In fact, they parallel judgements expressed by the US Army's Request for Proposal (RFP) that resulted in this SAI study. They are defined here, however, as fact corroborated by the SAI Threat Analysis described above. During the course of the study, SAI engaged these stated implications, so as to define potential targets and present recommended policy, planning mechanisms, organizational changes, and tactical considerations.

Appendix H to this report contains a discussion paper pertaining to the CONUS threat.

IV. CRISIS MANAGEMENT

Predicting a terrorist group's intentions, with any degree of accuracy, is dependent upon accurate intelligence. With the highly restrictive policies concerning intelligence gathering activities, the filing and retention of information, a capability to forecast or predict terrorist intentions with any accuracy does not exist. Even if this capability did exist terrorist acts could not be positively prevented. Rather, the probability for success would go down while the risk for the terrorist would go up. Without adequate intelligence there will be little leadtime, if any, leaving little specific forewarning of a terrorist attack or other disruptive activity. There must be a pre-determined plan for managing the crisis created by a terrorist attack and the plan must be able to be placed into effect as expeditiously as possible.

SAI has developed an overall U.S. Army structure for terrorist crisis management. It can be implemented with existing personnel and equipment. It goes on to consider the national and international implications of terrorism. This is due to the political overtones of most terrorist acts whereby reaction to the situation can involve the military and U.S. Government at every level - from the responsible individual at the scene to the President. The SAI developed crisis management structure covers:

- Incident reporting and transition to the terrorism crisis management structure.
- Terrorist crises occurring in the 50 U.S. states, territories, and possessions.
- Terrorist crises occurring on U.S. installations in foreign countries.

This crisis management structure, if adopted, could be implemented immediately at relatively little cost and is contained in Appendix B.

V. FIELD OPERATING/COMBATIVE ORGANIZATION/TACTICS

As stated earlier, terrorist situations include three (3) phases: pre-event, event, and post-event. Of the three, it is the event phase that includes the larger number of countermeasure actions and requirements that demanded extensive research and analysis. To this, SAI staff, isolated findings related to the event-phase in order to develop recommended organizational and tactical MODELS for use in creating procedures to counter terrorist acts on military installations. Findings, accrued through analysis of case studies and simulated, hypothesized terrorist situations, in addition to studies of TOE's/TDA's produced workable organizational concepts and tactics within a framework of realistic costs. Documentation of these findings are currently incorporated in a study component titled, "Field Counter-Terror Operations:

Organizational and Tactical MODELS" and is contained in Appendix C. This component focuses on the following event-phase matters:

- Task-Forcing/Organizing
- Command and Control
- Command relationships and problems of jurisdiction
- The Decision-Making process
- Intelligence collection, analysis and dissemination
- Negotiating
- Care and Safety of Hostages
- Tactics (assault . . . security)
- Communications
- Liaison with Media and Public Officials
- Support (logistics)

Below are highlights of the component's current directions:

Study of current U.S. Army capabilities balanced against an analysis of current and projected (1983) terrorist threats conclude that within assigned U.S. Army TOE/TDA law-enforcement organizations sufficient assets exist to form on-call counter-terror forces. To establish new force-structures and create additional permanent TOE-spaces would be to exaggerate the terrorist threat and underrate the capacity of military police units to implement countermeasures. This does not mean, however, that contingency plans for utilization of combat task-forces to counter the less-expected but more violent act should not be developed.

VI. AWARENESS-EDUCATION AND TRAINING

An overall program of education and training to create awareness of the terrorist threat and countermeasures has been developed and is contained in Appendix D. Pre-conceived notions, varied perceptions, and common misunderstandings tend to create unnecessary and unproductive actions or expenditure of resources. This point was illustrated in an article which appeared in the November 22, 1976 issue of the Washington Post extracted as follows:

"American Companies Act Against Terrorism in Iran

> American companies in Iran are taking steps to set up a joint defense against terrorism in a project promoted by the U.S. Embassy . . . There is nothing a company can do to isolate itself from terrorists no matter how much money it spends. The proposed security committee would be valuable if it raises the awareness of businessmen about terrorism and helps them to understand the motives and operational methods of terrorists . . . A tendency to rely on elaborate security systems that companies might be persuaded to install would be dangerous . . ."

The overall awareness program is two pronged with many facets of each. First, education of responsible individuals. The second major effort would be training individuals in physical security, and other specialties, and to train reaction teams. A combination of education and training appears warranted in order to achieve a well-balanced approach to countering terrorism - both before and after the occurrence of such an act or incident.

VII. INSTALLATION VULNERABILITY DETERMINATION SYSTEM

If one attempts to treat a military installation in a strict generic category, and design countermeasures accordingly, the result would be wasted resources in terms of money and personnel. It is obvious some installations are more vulnerable to terrorist activities than others. During the course of this study it was not practical, nor was there time or money, to survey and individually design countermeasures for each U.S. Army installation. Additionally, such individual surveys would be valid only at the time such a survey was conducted. Conditions change. Installations are opened and closed. What is needed is a measuring device which provides a continuous means for determining priorities or actions to be taken in order to reduce any installation's vulnerability to terrorist acts.

The purpose of the installation vulnerability determination system contained in Appendix E is to provide a comparative measuring device for the relative vulnerability of groups of installations to terrorist acts or incidents. It is intended to be used as a staff officer's analytical tool to establish priorities of actions, and allocations of resources, to reduce the vulnerability while at the same time conserve manpower and money. The more vulnerable installations should be directed to take certain actions, and be allocated resources as appropriate, to reduce vulnerability. It is unnecessary and impractical for all installations to be directed to take the same actions. This system has purposely been kept relatively simple, does not involve sophisticated calculations, or highly specialized personnel to use it.

To determine the vulnerability of any given installation, in the absence of a specific threat based on hard intelligence, ten major factors are considered. These are broken down into subfactors and degrees with a point value assigned. The major factors considered are:

- Installation characteristics and sensitivity
- Law enforcement resources
- Distance from urban areas
- Size of installation
- Routes for access and egress
- Area social environment
- Proximity to borders
- Distance from other U.S. military installations
- Terrain
- Communications with next higher echelon

It is readily apparent that any individual factor should not be a determinent in isolation of the other nine. There are obvious relationships between the factors. The system works on a scale of 0-100, whereby the higher the value the higher the vulnerability.

Again, this is a system that can be used in the absence of a specific threat based on hard intelligence (a condition that has proven to be unlikely). If a specific threat against a given target, or targets, were provided then specific countermeasures can be developed to meet that threat.

To establish the quantitative values for the major factors, two independent judgemental processes were used with a combining of these processes in order to provide a degree of conficence to the values used. First, the SAI study team, while developing the system, applied values based on its experience and judgement. Second, a group experiment was conducted. In selecting the group it was desired that the participants be in the military law enforcement field, have between 5 and 10 years service, and that they not have a current assignment to an installation. The officer's advance class, in an academic environment at the U.S. Army Military Police School, provided an ideal group. Out of 58 students participating, 50 valid responses were used to analyze and the 50 valid responses represented a total of 235 years of law enforcement experience. After analysis, the findings of the experiment were matched to the initial SAI values, and while no great disparities occurred, the SAI values were influenced and changed accordingly. The breakdown of the quantitative values is contained in Appendix E.

VIII. THE "INTELLIGENCE" PROBLEM

To ascertain existing strength, weaknesses and needs in the utilization of intelligence factors and assets, SAI staff studied intelligence support organizations, directives and operations, and conducted interviews with officials functioning in intelligence positions. Analyses of terrorists events, and the intelligence or lack of intelligence preceding these events, were also conducted. Overriding throughout was an obvious and often-stated conclusion: "Adequate intelligence is one of the highest priority requirements in preventing and coping with terrorism."

Two other matters, which place constraints on development of effective intelligence, are as follows:

- The Privacy Act of 31 December 1974 has limited agencies' ability to protect records pertaining to individuals, as defined by 5 USC 552a (a)(2), which are generated during the course of conducting the business of the agency. While Federal law enforcement agencies have been exempted from disclosure of the information itself, as well as many other provisions of the Act with the approval of the agency head, the mere acknowledgement of the existence of a record may be sufficient basis for the individual to compromise its value, initiate litigation and hamper the agency's efforts to corroborate and prevent a criminal act. EO 11905 (February 1976) has placed constraints on intelligence gathering leading to concern that valuable information on terrorists may be denied those tasked with the responsibility for countering radical acts of violence.
- There are indications that DOD and DA directives and regulations which serve as implementors of the above "Act" and "Order" have been misinterpreted at field levels, that is, restrictions on intelligence collection have been exaggerated, in some cases practically eliminating the intelligence collection effort.

A more detailed explanation of the intelligence problem exists in an analysis prepared by this contract's Principal Investigator, Mr. Rowland B. Shriver, Jr., advanced copies of which were forwarded to some members of the Study Advisory Group through the COTR. This paper is provided herewith as Appendix F.

IX. REVIEW OF REGULATIONS AND POLICY

During the course of the SAI study there were comprehensive reviews of regulations and publications, both in effect and in draft, promulgated at various levels of command. At Appendix G are comments on some of the most pertinent directives, particularly the Draft DoD Handbook 2000.12, Subject: Protection of Department of Defense Personnel Against Terrorists Acts. In addition, assistance was provided in developing Army Regulation 190-XX, SUBJECT: Countering Terrorism and Other Major Disturbances on Military Installations. This new regulation and an associated DA Pamphlet and/or Field Manual incorporating policies and procedures developed during this study should provide the Army with a strong program for countering terrorism, and other major disruptions, on its installations.

X. RESEARCH AND DEVELOPMENT

The U.S. Army Material Development and Readiness Command (DARCOM) uses a system of project managers to manage major research and development programs. There are approximately 58 such project managed weapons/equipment systems. These are, for the most part, major items to improve the combat capability of the Army. Law enforcement equipment is not included within any of the major research and development programs primarily because of relatively small dollar cost of individual items and its primary purpose does not contribute to enhancing combat readiness.

The International Association of Chiefs of Police (IACP) is establishing standards for items of commercial law enforcement equipment. Rather than embarking on a major, independent and expensive development program, the Army should use the standards established by the civilian law enforcement sector. This technological transfer from civilian to military has obvious monetary advantages.

The U.S Army Military Police School should develop revised Common Table of Allowances reflecting law enforcement equipment standardized by the IACP and determined to be suitable for military law enforcement purposes.

Installation Provost Marshal should review the installation Tables of Distribution and Allowances to determine commercial items of law enforcement equipment for inclusion and would be tailored to the needs of the specific installation. This would then provide a basis for programming and budgeting for local procurement.

XI. MISCELLANEOUS

Appendix H contains various documents that were developed during the course of the study. They are included in the final report as they provide additional insight to the comprehensive research that was conducted during this study. These documents are:

- Perceiving the Terrorist Threat in CONUS. This paper treats (1) characterizations about US terrorist groups which can be drawn from their current period of silence, and (2) a constraint placed upon law-enforcement and other agencies in the U.S. which precludes development of accurate terrorist intent prior to an act.

- Summary of Field Visits - During October and November 1976 the SAI study team made visits to the following U.S. Army installations:

  Fort McNair, Washington, D. C.
  Seneca Army Depot, New York
  Fort Rucker, Alabama
  Fort McLellan, Alabama
  Fort Bragg, North Carolina
  USAREUR, Heidelberg, Miesau, Kriegsfeld and Frohn-Muhle

These visits proved to be invaluable in collecting information, personal views concerning counter-terrorism, and absorbing the nature of the problems faced by responsible individuals at installation level. This "grass roots" input was vital in the formulation of realistic policies, concepts, and methods to counter terrorism on military installations. A general observation concerning the visits was that the outstanding cooperation and interest displayed by those individuals contacted greatly enhanced this information collection effort. Another overall observation is that many excellent individual efforts are being made to cope with the problem but all seemed to be looking for a total coordinated Army program. The highlights of each visit are contained in Appendix H.

- Aliens in Nuclear Duty Positions. A finding that resulted from a visit to an installation was considered to be sufficiently serious to warrant immediate reporting along with recommendations for corrective action. A memorandum dated 26 October, 1976, Subject: "Aliens in Nuclear Duty Positions" was provided the Contracting Officer's Technical Representative and a copy is contained in Appendix H.

- Survey Questionnaire - Preparatory to evaluating the vulnerability of U.S. Army installations, and developing possible changes in policies, SAI personnel made visits to selected installations both in CONUS and Europe. Due to budgetary and time constraints it was not possible to make as many visits as considered necessary to gain a good sample. Consequently, the Study Advisory Group recommended a survey questionnaire be developed and sent to certain installations. The questionnaire was prepared; however, unforeseen staffing difficulties precluded sending the survey to the selected installations. As a result, it was decided to prepare the survey for presentation to the attendees at the Law Enforcement Conference held at the U.S. Army Military Police School, Ft. McClellan, Alabama 1-3 March 1977.

While only 12 responses (approximately 17%) were returned for analysis it is believed that it represents a valid sample. This view is based on the wide variance of current law enforcement responsibilities of the respondents. It should be noted that not all respondents addressed every question which accounts for the variance in the number of responses to each question shown in Appendix H. While each reader of this report can draw his own conclusions by reading the detailed responses to the survey questions at Appendix H there are some overall impressions summarized below.

- There is a wide variance in perception of the terrorist threat to Army installations.
- There is a divided opinion on the role of Military Police versus CID in responding to acts of terrorism.
- There is general agreement on lack of policy guidance in countering terrorism.
- There are varying degrees of emergency plans developed at installation level.
- There appears to be a lack of understanding, or appreciation, of jurisdictional problems associated with acts of terrorism.
- There is little or no appreciation that an actual terrorist act on a military installation can be escalated quickly to the national level rather than being contained at the installation.

XII. RECOMMENDATIONS

Based on the results of this study, it is recommended that:

- A policy statement delineating terrorism as a crime, and coping with terrorism a law enforcement function be issued. The DCSPER (DAPE-HRE) should be designated as the DA staff element responsible for coping with terrorism.

- Department of the Army consider initiating action to update the existing Memorandum of Understanding between Department of Justice and Department of Defense, with emphasis on jurisdictional and support responsibilities during terrorist crises. This then would serve as a basis for local agreements between installations and FBI field offices, a requirement which should be dictated by Army Regulation.

- The crisis management plan (Appendix B) be implemented as soon as possible after required staffing and coordination.

- The Organizational and Tactical Models for Field Counter-Terror Operations, contained in Appendix C, be incorporated in a Field Manual.

- The Awareness Program, contained in Appendix D, be implemented by Training and Doctrine Command.

- The Installation Vulnerability System, contained in Appendix E, be considered for use as a tool for staff planning.

- The U.S. Army Military Police School develop revised Common Tables of Allowances reflecting commercial items of law enforcement equipment standardized by the International Association of Chiefs of Police, and determined to be suitable for military law enforcement purposes.

- All installation Provost Marshals review the installation Table of Distribution and Allowances to determine commercial items of law enforcement equipment for inclusion, tailored to the needs of the specific installation.

- The case study concerning aliens, contained in Appendix H, be forwarded to the Assistant Secretary of Defense (Comptroller) with a recommendation that DoD Directive 5210.42, "Nuclear Weapon Personnel Reliability Program" include a requirement that an individual must be a U.S. citizen to qualify for entry into the Personnel Reliability Program.

- The Service Secretaries and Commanders at all levels should institute a comprehensive review of all policies, directives, and regulations responsibilities of - and restrictions placed upon - intelligence gathering agencies to remove "safe-siding" that inhibits exercise of full investigative/intelligence authority authorized by the Privacy Act and Exec Order 11905.

- Commanders at all levels should require of their intelligence agencies the positive execution of intelligence activities authorized under the Privacy Act and the Executive Order, monitor compliance and punish individual abuses.

- A comprehensive study should be accomplished which evaluates the present restrictions on intelligence gathering with the objective of submitting new legislation, if appropriate, permitting the gathering of intelligence sufficient to protect society while protecting individual rights.

APPENDIX A

THREAT ANALYSIS

I. INTRODUCTION

A. General

Analysts point out more terror occurs in summer than winter, that specific events trigger increases, but to predict a day and a target for it is impossible without "street" intelligence. SAI has not attempted to develop a calendar of future terror, but instead realistic deliverables - measured probabilities based on inputs which uncover decidedly that terror will/or will not occur in the broad sense, at what intensity levels, and in what form.

B. Scope

1. Framing. Behind this analysis is a need to develop feasible alternatives for US Army countermeasures against terrorism. Of the incidents between 1968 and 1976, less than ten percent occurred on US military installations. If SAI were to focus only on these, there would be insufficient data to develop probabilities. Thus, other places where terrorists have acted served as base-line areas for study. Metropolitan pockets of the US, Western Europe, the Middle East and Latin America have had terrorist activities that offer wide spectrums of information applicable to probable events on US Army installations.

Today, there are more than 140 terrorist groups. To analyze each is pointless. It is unlikely certain terrorists will impact on US Army installations, and in their actions not a great deal can be learned that cannot be learned through study of others. Terrorist organizations this Analysis deals with are those which acted upon US Army installations and those which have not, but have gained recognition worldwide as effective terrorists, whose actions and characteristics provide data for learning the state of the art - motives, objectives, modus operandi.

This analysis covers geographical spectrums of terrorist acts, which are -

- Global
- Regional (hemispheric, e.g., terror in Latin America, or the Middle East)
- National (a single country)
- Local (a city or county)
  - urban
  - rural
- Installations
  - DoD
  - Other US Government
- Targets
  - material (buildings, houses, aircraft)
  - human

2. Defining. In readings on terrorism, the lack of common definition for repeatedly-used terms is evident. Terror, Terrorist — words used frequently —have different meanings as used by different government officials. A need for standardization exists, so that SAI and those who would extract value from this Analysis could perceive descriptive terms in much the same way. Part III, this document, includes a glossary of terms.

3. Selecting. It would seem impractical to begin this project without first sorting out subject-components. What is terrorism in terms of objectives or events that cause it to exist? The question assisted SAI in recognizing one type terror from another, especially in categorizing them for study. Types of terror are explained in Part IV, Overview and Findings.

4. Qualifying. Each major CONUS and OCONUS terrorist group has been assessed to develop whole capability structures from which probability factors evolved. This document profiles groups. Part IV, Overview and Findings, discusses activity patterns and potential for new violence.

5. Quantifying. Part IV also includes data summaries, or, statistical analyses of terror phenomena. Understanding the terrorist threat can be achieved through study of tables presented.

C. Approach

1. A four-sided relationship field matching (a) terrorist organizations to (b) areas of operations, to (c) frequency of activities to (d) terrorist objectives, was used to determine which geo-political locations and what terrorist organizations should be studied. Once selected, each location and organization was evaluated in a framework of relevance to probable type terrorist actions against military installations. Those with little or no application in this frame were eliminated.

2. Selections, "Inputs". Threat information needs were ascertained by relating terrorists to targets and to ultimate objectives. Immediately recognizable were categories such as motivation, and resources and tactical capabilities. Within these categories, subsets of information - requirements grew evident. Selected for examination were goals and objectives, preferred strategies and tactics, significant past operations and operational trends, current status, strength, available technology.

3. Subject Matter Experts. In addition to collection, collation and analysis of written material, SAI visited officials and analysts of DoD and other government agencies concerned with problems of terrorism. These persons represented US Department of State; the Central Intelligence Agency; Office of the Assistant Chief of Staff for Intelligence, US Army; Office of the Criminal Investigation Division Command, O-DCSPER, US Army; major CONUS/OCONUS installations, US Army; Office of Chief of Engineers, US Army; the FBI; and the Federal Aviation Administration. A wealth of data and capability judgements were obtained in this manner.

4. Analysis. The metamorphisis from raw data to conclusion involved analytical travel points. This phase of the analysis demanded the most effort. The analytical points were used to synthesize data and determine outcomes for various threat factors, terrorist groups, types of terror, and of terror as aggregate phenomena impacting globallv, regionally, nationally, and upon US Army installations.

5. Constraints. The recent Privacy Act denies active investigations of individuals (citizens or legal aliens) or US organizations inclined toward terror until a specific act to which they can be related has occurred. This inability, on the part of USG and US Army law enforcement and intelligence-gathering agencies, to develop information on terrorists prior to the deed can now and in the future hamper legitimate actions. Still, unofficial and overt accounts by journalists and subject matter experts allowed SAI to piece together trends and patterns, although a greater abundance of data would have provided a more precise set of probabilities.

Glossary

a. Language peculiar to the study of terror has formed. Government, military and private sector analysts designed terms and phrases which appear in documents and articles building today's terror bibliographies. But there are no universally-accepted definitions. The US Department of State characterizes terror differently than the US Army. For example, International Terror appears to have special meanings in CIA studies which differ from meanings elsewhere.

b. To insure readers understand what is meant by terms used repeatedly in this Analysis, a glossary is provided.

c. Terms

1. Terrorism - In the broadest sense, terrorism may be defined as follows:

> "An act, or acts, against human and/or material targets by a person or persons to instill fear, obtain demands, and/or destroy property or lives."

In the political objective sense, terrorism is more appropriately defined as:

> "The calculated use of violence or the threat of violence to attain political goals through instilling fear, intimidation or coercion. It usually involves a criminal act often symbolic in nature and intended to influence an audience beyond the immediate victims." (This definition is much used within U.S. Intelligence Community.)

2. Terrorize - ". . . to conduct terror according to a plan."

3. Terrorists - "malcontents who conduct terror as planned."

4. Terrorist Groups or Organizations - "groups or organizations that select the uses of terror to achieve objectives."

5. Threat (as in THREAT analysis) - "terror in selected environments qualitatively and quantitatively defined."

6. Threat - "an inference, based on more than speculation, terror will occur."

7. Transnational Terror - "such action when carried out by individuals or groups controlled by a sovereign state."*

8. International Terror - "terror planned and executed by groups operating beyond national boundaries." The U.S. Intelligence community usually defines international terror as "terrorism transcending national boundaries in the carrying out of the act, the nationalities of the victims, or the resolution of the incident. These acts are usually designed to attract wide publicity to focus attention on the existence, cause, or demands of the terrorists. "

9. Cooperative Terror - "terror carried out by one group to support the aims of another."

10. Domestic Terror - "terror executed within a particular nation's boundaries by indigenous terrorists based therein."

11. Urban Terror - "actions in cities or metropolitan areas."

12. Rural Terror - "actions in small town or countryside.'

* CIA definition, see CIA Research Study, International and Transnational Terrorism: Diagnosis & Prognosis, April 1976

13. Counterterror - "acts that reduce or prevent terror."

14. Countermeasures - "methodologies, programs, plans, organizational activities and anncuncements designed to reduce if not prevent terror."

15. Pathological Terror - "that which is carried out by mentally disturbed persons."

16. Vengeance Reaction Terror - "that which is carried out by individuals against others whom they believe to have antagonized or deprived them."

17. Spontaneous Terror - "that which is carriedout as immediate response to fear or failure. Example: Bank robber taking hostages while fleeing scene of crime."

II. OVERVIEW AND FINDINGS

Overview. This assessment is about terror, specifically (1) its uses as a coercive and disruptive instrument to create situations favorable to aims of terrorists, (2) the capabilities of certain groups and individuals to employ terror now and in the future, in turn, (3) the impact of terror probabilities on the U.S. Army, CONUS and OCONUS.

There are more than 140 terrorist groups operating in around 50 countries, roughly 20 in the United States. Since 1968, these groups have been responsible for nearly 1,200 incidents resulting in over 800 deaths and more than 1,700 casualties.

Major terrorist groups operating outside the United States are listed on the following page.

GROUP	TERRITORY
Ai-Fatah	Middle East
Arab Liberation Front	Middle East
Army of National Liberation	Columbia
Baader-Meinhof Remnants: ● 2 June movement ● Revolutionary Call	FRG
Black June	Middle East
Black September (sponsored by PFLP)	Middle East
"Carlos" group	W. Europe/Middle East
Erritrean Liberation Front	Ethiopia
ERP (People's Revolutionary Army)	Argentina
IRA-provisionals	Northern Ireland
JRA/Japanese Red Army	Japan
Lotta Continua	Italy
Montoneros	Argentina
Movement of National Liberation (MLN/Tupamaros, less effective now than in 1960's)	Uruguay
Movement of the Revolutionary Left	Chile
People's Liberation Front	Ethiopia
Popular Front for the Liberation of Palestine (PFLP)	Middle East
Red Brigade	Italy
Turkish People's Liberation Army (TPLA)	Turkey
23rd of September League	Mexico
UDA/Ulster Defense Association	N. Ireland

United States terrorist groups active, or inactive but still assembled are -

GROUP	TERRITORY
Deleted per AR 380-13	NY and SF
	San Francisco
	Miami
	NY - Puerto Rico - California
	NY
	SF
	Los Angeles
	SF
	SF
	San Diego
	Oakland, SF, Los Angeles
	South
	NYC/Chicago

In Western Europe, remnants of the Baader-Meinhof gang are anarchist, while Italy's Red Brigade is Marxist. In some cases, there are no political causes motivating terrorists. Al-Fatah, Black September and the recently active Croatian emigre group serve nationalistic/ethnic causes.

In all cases, objectives of terrorist groups are connected to belief-systems that fall within basic realms of human concern. These characterizing realms are -

- politics
- ethnicity/nationalism
- religion
- the environment/ecology
- personal gain (mercenaries)
- pathological need

Within these realms, division is evident. Among political groups, distinct and polarized types have been -

- left
- extreme left
- reactionary
- extreme reactionary
- anarchist

Continued examination splits political groups further. Among left and extreme left are found groups that are -

(left)

- Soviet-Marxist (accepting doctrine on terror designed by Soviet Union - "politics before violence.")
- Trotskyite (revolution when military climate is favorable)

(extreme left)

- Maoist ("politics grows from the barrel of a gun")
- Castroite/Guevarist ("revolution begins with physical action - uprisings")

Among reactionary and extreme-reactionary groups are found -

- Fascists
- Vigilantes (favoring existing governments)

Following is a breakout, in terms of objectives and belief-systems of political groups:

(OCONUS) GROUP	CREDO
Baader-Meinhof Gang (FRG)	Anarchist
ERP (Argentina)	Marxist
JRA (Japan)	Maoist
PFLP (M.E.)	Maoist
Red Brigade (Italy)	Marxist

(CONUS) GROUP	CREDO
Deleted per AR 380-13	

Ethnic and Nationalistic Groups also have classifications. These are --

(1) those operating in a country that is their legal habitat;
(2) those operating outside their legal habitat to effect change within;
(3) those operating outside a country not their legal habitat but which they desire as such.

Operating ethnic and nationalistic groups within the above classifications have been -

(OCONUS)

GROUP	TYPE
Al-Fatah (Middle East)	(3)
BSO (Middle East)	(3)
IRA (Northern Ireland)	(1)
PFLP (Middle East)	(3)

(CONUS)

GROUP	TYPE
Deleted, AR 380-13	

Some ethnic and nationalistic groups also have political objectives. For example, the IRA-provisionals are Marxist in their political belief, and the PFLP is Maoist. However, their ethnic and nationalistic goals are over-riding.

Religious groups are few. The IRA falls within the religious and is made up of Catholics who, perceiving discrimination, conduct acts against targeted Protestants. In this aspect, the IRA is unique and three-pronged. As terrorists, they are political (establish a Marxist government), also ethnic and nationlistic (eliminate from Ireland all British controls), and religiously motivated as well (exit from Northern Ireland any Protestant domination).

Groups perpetrating terror to effect environmental or ecological situations are few. Recent examples include threats to damage or destroy nuclear facilities.

Mercenary groups, or individual mercenaries, are few, although there exists a polyglot of contacts and hiring organizations that could supply large numbers of mercenaries to rich buyers anywhere in the world. At present, the "Carlos" Group is the only mercenary terrorist organization that has impacted on world or national order. Politically Marxist, this Group has conducted operations primarily for money. The group is often cited as "ideological mercenary."

Rarely a group characteristic, pathological need terror is not to be ignored. Records maintained by the USG's Federal Aviation Administration (FAA) reflect a high proportion of skyjackings conducted by mentally disturbed individuals.

Individuals who conduct terror from pathological need have been -

- psychotics, or -
- neurotics driven by extreme stress

Employment of Terror. Terror is employed by terrorists to achieve (1) objectives toward obtainment of future goals, and (2) immediate goals. Examples of the former are -

- acts to lay groundwork for dramatic changes in government, coups d'etat, revolution, civil war, or war between nations
- acts to turn the tide favorably during guerrila warfare
- acts to influence national or international policy decision-making

Examples of immediate goals: acts to:

- obtain worldwide or national recognition for "cause"
- take life (assassinations)
- cause government over-reaction and repression, leading toward immediate public dissension.
- harass, weaken or embarrass military or other security forces
- obtain money or equipment
- disrupt or destroy facilities or mobility and communication lines (e.g., to deny forms of energy)
- prevent development of new facilities or mobility and communication lines
- demonstrate power or tactical credibility
- prevent imminent executive decisions or legislation
- cause strikes or work slow-downs
- discourage impending foreign investment or foreign government assistance programs
- express religious, ethnic or racial prejudices
- influence elections
- embarass and weaken reputations and political positions of public leaders
- free prisoners
- satisfy vengeance (often, assassinations)
- build or sustain morale within terrorist group
- demonstrate commitment to "cause"
- express sheer frustration
- express pathological need (as committed by mentally disturbed)

Characteristics of terror are -

- terror, as stated repeatedly by analysts, is "theatricality for effect".
- the primary "effect" desired by terrorists is fear.
- in balance, terrorists are weaker than opposing military or security forces, or "target governments", until sufficient fear is aroused.
- during acts of terror, victims are not necessarily related to "target governments" or "target audiences". A kidnap victim, or persons taken hostage and barricaded, may in no way be related to those from whom the terrorists desire to exact political, social or military decisions, or money and equipment.
- a terrorist operation can be highly successful even when perpeterators have been killed, wounded or captured. That is, tactical success and mission success need not be related. If most of a team of terrorists are killed during an operation that has gained worldwide attention, the terrorist group's command element may consider the operation highly successful, especially if "publicity" was the main terrorist objective. It is dangerous for legitimate governments to believe a successful counter-terror campaign is in the making only because terrorists have suffered tactical and manpower failures. The BSO considered its Munich Massacre a success, even though none of the terrorist demands were met, and hostages and seven of nine terrorists were killed.
- political terrorists are rarely suicidal.... they expect to succeed in their mission unharmed......

- terror can be effective violence by revolutionary organizations that wish to wage guerrilla warfare in densely-populated urban areas.

- because of advanced transportation and communications technology, terrorists can be highly mobile and strike almost anywhere.

- terror is cheap . . . few perpetrators with inexpensive small arms can create disruptions affecting whole nations.

The degree of fear instilled by terror normally parallels the intensity of the drama associated with the terrorist act. Nuclear theft would, of course, create more fear than theft of conventional small arms.

According to terrorist theory, fear leads to achievement of demands. If enough people fear terrorists would use a stolen nuclear device, chances terrorists will receive payment-on-demand are greater.

Fear of terrorist action, as threatened, reduces the effectiveness of security forces almost proportionately until either -

- security forces can neutralize the object of the fear (in case, a stolen nuclear device . . . another case, threats to kill hostages, wherein security forces would have to free them by force or through negotiations); or:

- security forces, or "target governments", can reduce the credibility of the terrorists to effectively do what they have threatened (e.g., proving the terrorists are bluffing and will not, under any circumstances, "back their play"); or:

- "target governments" can convince the "target audience" (population) to accept the consequences of the act terrorists have threatened, thereby eliminating fear with stoic acceptance (probably impossible in extreme cases), closing the door on negotiations.

Transnational, International and Domestic Groups. CIA, Research Study, International and Transnational Terrorism: Diagnosis and Prognosis, April, 1976 (unclassified), defines: transnational terror as "such action when carried out by basically autonomous non-state actors", meaning they are in no way controlled or directed by one or more governments, although they may receive government assistance. CIA explains further that transnational groups conduct operations in more than one state or region. The PFLP (Popular Front for the Liberation of Palestine) is a transnational group.

A prediction emerges weighing transnational groups against those international and domestic. International groups are controlled by sovereign states. A domestic group is autonomous, operating in one country. Uruguay's Tupamaros were, in the sixties, domestic. For governments utilizing an international group, surrogate warfare may be an objective. Today, and in the near future, this would be high-risk adventurism on the part of any government. Backlash from other governments would be disastrous. Big powers would not risk detente, nor would smaller nations risk big power invervention. Even a constituency of smaller nations would consider international terror unfavaorable. Violence by proxy, twice-removed, via the clandestine offerings of assistance to a transnational rather than an international group has less risks. Increases in terror are more likely to be transnational.

Some governments support transnational terror opting for current or future political and military leverage. For example, the Soviet Union has provided training and logistics support to PLO terrorists and to leaders such as Illich Ramirez Sanchez ("Carlos") who attended insurgency training courses at Patrice Lumumba University in Moscow. Cuba has trained more than 300 persons who are now Latin American terrorists. Libya has supported the PFLP and the "Carlos" Group with money and arms, and acts as a safe-haven for hijackers.

Among transnational groups are the BSO (Black September Organization), the PFLP (Popular Front for the Liberation of Palestine), ana tne JRA (Japanese Red Army). Cooperation among these groups has grown from mutual assistance, engendered by ideological similarities, to that stimulated by necessity, or "need to survive". The JRA finds it difficult to conduct operations in Japan due to government crackdowns, thereby conducts acts outside the parent country. To do so, support from groups oustide Japan is necessary. The PFLP, losing support in Lebanon, no longer able to launch as many operations in Israel, may increase acts in other parts of the world.

When routed from one base to another, transnational groups lose self-reliance. Dependency on others, to supplant resource and operational weaknesses, is already a trend. In Latin America. Argentine, Chilean and Bolivian once-domestic terrorist groups have formed a "Junta", a directorate with organizational characteristics bordering on the formal. Several Middle East terrorist groups grew under the umbrella of a formalized PLO. Cuban exile groups are connected through an administrative council. It is possible transnational groups operating cooperatively in Western Europe can escalate from the "informal" to the "formal", developing an umbrella mechanism. A directorate of terrorist groups, however, alone would not indicate new terror. Rather, terror would be more carefully planned, sufficiently supported, and conducted by personnel selected from a larger array of experts. From this, probabilities for successful operations are greater. In 1972, members of the JRA (Japanese Red Army) joined members of the PFLP to conduct the LOD Massacre. In 1976, a member of the Baader-Meinhof Gang (FRG) participated in the Entebbe incident.

Development of a "directorate" in Western Europe would be slow. Although dependency-needs among its groups are high, internal dissension in most over leadership, operational targets, modus operandi and resources is also high, obviating quick resolutions through creation of an umbrella mechanism. Unless forced by social or political events, today's West European terrorist groups should remain decentralized for some time.

Summarily, international terror - that by legitimate governments - does not pose as serious a threat as transnational terror - that by autonomous non-state groups. Transnational terror will continue at present levels, or slightly higher, and because of formalizing cooperation among groups realize an increase in efficiency of operations.

Findings

1. Size and Composition. The larger terrorist groups exist outside the United States. Erritreans, Al-Fatah, and the IRA are largest. Size, however, does not necessarily mean greater frequency of operations. Organizational growth presents new administrative and support burdens, minimizing ability to insure additional terror. When the Baader-Meinhof Gang conducted its series of violent incidents, there were hardly fifty members.

Certainly, a small group can increase frequency of operations, but only to a point; minimum personnel do so much. When small groups become larger, frequency of operations reach a similar point, as growth impacts on operational capability adversely. Procurement, storage and use of resources, ability to communicate, security -- these necessities become burdensome with size. Al-Fatah terrorists operating in Jordan (1969-70) grew so rapidly, Arafat lost control of them. This helped precipitate decimation of more than two-thirds of Al-Fatah by King Hussein. In Italy, the Red Brigade has grown in strength, but it does not conduct the hard, shocking terror smaller groups can. In Uruguay, when Tupamaros grew, the coloration in which lay their popular support changed. Small, they were p·rceived as "Robin Hoods". Large, they were viewed as bureaucratically-styled murderers.

Larger groups a·e exposed sooner or later. The bigger the organization, the thinner the security shield. Governments respond ·y increasing reprisal forces, escalating conflict to stages terrorist groups may be unable to handle. Venezuelan, Brazilian and Guatemalan counterinsurgency models of the sixties are examples of this occurrence.

Terrorist groups know the advantages of smallness. The larger group can only succeed for the long term in a weak political environment. When such an environment exists, terrorists have an operational area conducive to guerrilla warfare. Here, terrorists become a guerrilla force, and terror a component of the guerrilla war. In the fifties, in South Vietnam, Viet Cong began as terrorists.

In the Federal Republic of Germany (FRG), where the political structure is stable, a large terrorist group could not survive. Individual expansions of terrorist groups are probable in some regions, not so in others. On a one-to-ten scale (ten highest probability, zero lowest) a rough outlook regarding potential for increased size is -

REGION	PROBABILITY
Western Europe	2
Middle East	3
Northern Ireland	4
United Kingdom	1
Latin America	3
Asia	1
United States	0
Africa	6

Assigning low probabilities to growth of individual groups in no way implies there will not be an increase in terror. They state groups will be cautious about physical development. Nor do they imply these groups will be any easier to contain. Further, growth does not, as a variable, reflect anything about creation of new groups, or about coalitions of groups that currently exist

By size, major groups rank as follows -

(OCONUS)

GROUP	APPROX. SIZE
Eritreans (Ethiopia)	10,000
Al Fatah (M.E.)	8,000
Tupamaros (Uruguay)	200
ERP (Argentina)	600
PFLP (M.E.)	300
IRA (N.I.)	1,000
"Carlos" Group	50
Baader-Meinhof Remnants (FRG)	40-50
JRA (Japan)	25
BSO (M.E.)	60

(CONUS)

GROUP	APPROX. SIZE
Deleted, AR 380-13	

2. Composition. The organizational make-up of a terrorist group is determined by several factors. Significant are -

- security, and
- strength (personnel)

Any illegal organization with a weak security shield is penetrable and will not survive. Strength must be managed and controlled by appropriate organizational lines. Affecting security and strength are -

- effectiveness of government counter-terror forces,
- degree of popular support, and
- internal communication capabilities.

Counter-terror forces, when effective, penetrate terrorist groups and destroy from within, or track terrorists down, or keep them so employed in defense and security that mobilization for new terror is impossible. To avoid effective counterterror, terrorist groups must be extremely covert. Traditionally, the clandestine cell has been the building block upon which these groups form and survive.

Reliable popular support acts as an outer security shield, a buffer between terrorists and the government, allowing them to move about more freely. Its greatest attribute lies in the network of safe-houses popular support provides. The safe-house is where terrorists not only hide, but plan, communicate, train, manufacture and store weapons and explosives, and rehearse.

It is common knowledge terrorism does not succeed without sufficient popular support. Mao's "Fish in the Sea" principle applies as much to terrorists as to guerrillas. Popular support also aids terrorists in transporting personnel and equipment, identifying and reconnoitering targets, and in acquiring daily provisions. Group structure is affected by how much of this support exists. Greater support allows for larger and more numerous cells, and closer union between them.

Internal communication capabilities are among determinants of security and strength requirements. Secure equipment alleviates the need for excessive message drops, meetings, and cut-outs. Effective communication of this sort prevents groups from having to create special cells, or sub-cells, to provide these communication values. In any underground operation, "communication" affects time, manpower, resources, location of cells and safe-houses, operational targets and tactics. Thus, the structural lines of a covert terrorist group must be compatible with communication capabilities.

Today, no terrorist organization operates where counterterror forces are so ineffective, where popular support is in such abundance, or where communications are so effective, that as groups they can act freely at all times. Most have to be covert continuously. In the Middle East, however, Al-Fatah and the PFLP often conduct open meetings and can move about in certain areas with minimum security because of extensive popular support. Their once-deep cells now function along with others overtly. In the FRG and Japan, remnants of the Baader-Meinhof Gang and the JRA, respectively, can function only in the most stringent clandestine ways, through cells whose members do not know the whereabouts of members of other cells.

Following is a list of groups in relation to above-described factors -

a. Effectiveness of Government Counter-Terror Forces (high, moderate, low; based on reports of government security forces/historic data).

(CONUS)

GROUP	RATING
Al-Fatah	Low
Baader-Meinhof Remnants	High
BSO	Low
ERP	Moderate
IRA	Moderate (UK) Low (Ulster)
JRA	High
PFLP	Low

(CONUS)

In the United States, no terrorist group has succeeded in developing an effective long-term campaign, although some have operaterd helter-skelter for years, one since the Truman administration.

b. Degree of Popular Support (high, moderate, low; based on government and private sector reports, studies/historic data).

(OCONUS)

GROUP	RATING
Al-Fatah	High
Baader-Meinhof Remnants	Low
BSO	Moderate
"Carlos" Group	High - only in Middle East, Low, elsewhere
ERP	High
IRA	High
JRA	Low
PFLP	High
Red Brigade	Moderate

(CONUS)

No terrorist group in the United States enjoys sufficient popular support for a campaign of terror.

c. Internal Communication Capabilities (excellent: modern equipment, trained operators, or perfected system of drops, cut-outs, runners; fair: sufficient but troublesome equipment, some but not enough trained operators, marginal system of drops, cut-outs, etc...poor: no equipment, ineffective system...)

(OCONUS)

GROUP	RATING
Al-Fatah	Excellent
Baader-Meinhof Remnants	Fair
BSO	Excellent
"Carlos" Group	Excellent
ERP	Excellent
IRA	Excellent
JRA	Fair
PFLP	Excellent
Red Brigade	Fair

(CONUS)

No terrorist group in the United States is known to have sophisticated communications equipment, although most have a perfected system of drops, cut-outs,runners that can be rated excellent.

Relationships among the above factors indicate the closeness between effects on security and strength and organizational structure. Groups rated high in two or more areas are also those which have rigid organizational lines irrespective of overt behavior of sub-elements at territorial bases, and which have been more successful.

Organizations that enjoy high popular support, have excellent communications, or are not always confronted in immediate environs by effective counter-terror forces are -

(OCONUS)

GROUP	COMMENT
BSO PFLP Al-Fatah ERP	Each of these groups is highly cellularized, maintains separate tactical and support forces, enjoys much popular support and has modern

COMMENT

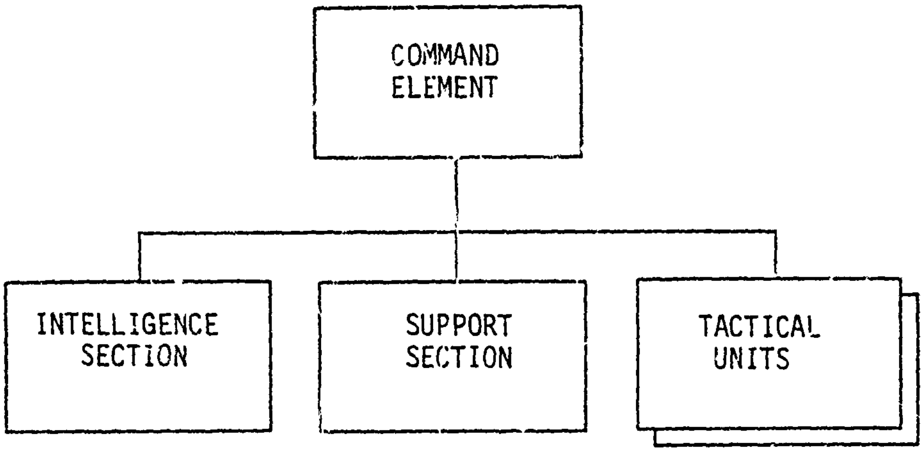
signal equipment, trained operators, and perfected human systems. Among terrorist groups, they are most formidable.

(CONUS)

In the mid-sixties, certain elements of the US "left" participated in the upkeep of an underground that harbored or moved wanted terrorists, dissidents, draft-evaders and deserters. Remnants of this underground still exist, aiding US terrorist groups. The ability of this quasi-underground to assist terrorists is enhanced by democratic freedoms in the US that allow persons to travel unchecked except at borders and in airports. The US also includes inexpensive transportation, and highly urbanized areas where persons melt easily into populations. This provides US terrorists a thick security shield, behind which they communicate effectively and receive support from sympathizers for continued survival if not for active operations. By no means, then, can US left-wing terrorist groups be written off as elements that do not enjoy some degree of support, or which communicate ineffectively. These factors have allowed terrorist groups to sustain cellular organizations.

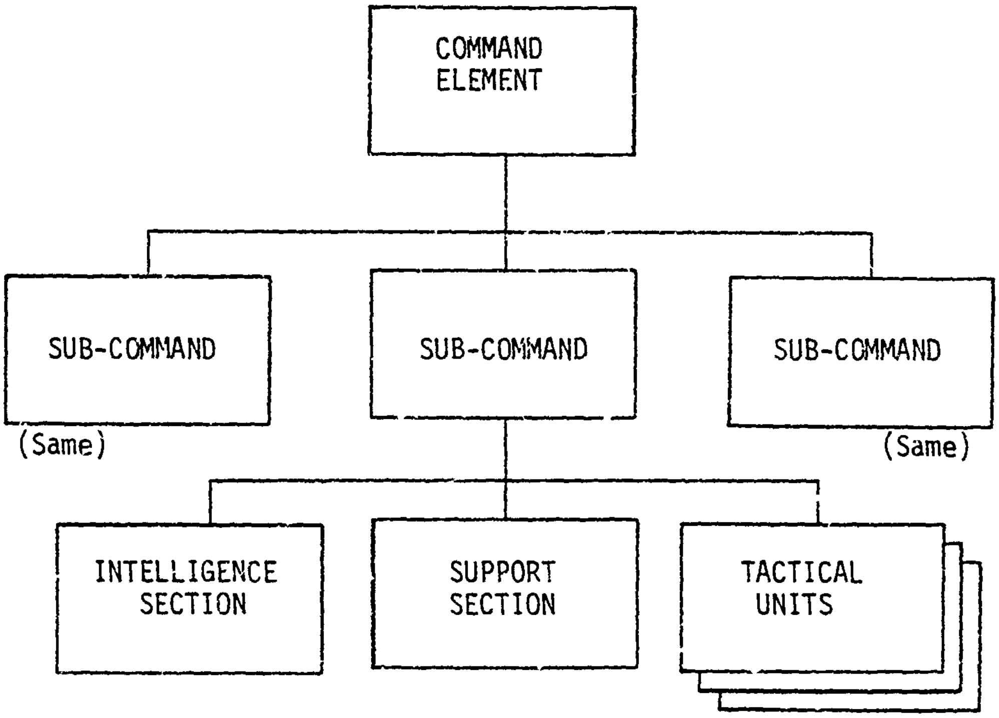
As stated, in OCONUS and CONUS, terrorist groups exist along covert organizational lines. The smaller terrorist group (less than 100) has a command element, support section, intelligence section, and two to five basic tactical units comprising two or three cells, or teams, each with two to five persons. The larger group has a command element, and several area and/or sub-commands controlling perhaps three to five tactical units, support section, intelligence section. Examples are -

(typical smaller terrorist group, 40-50)

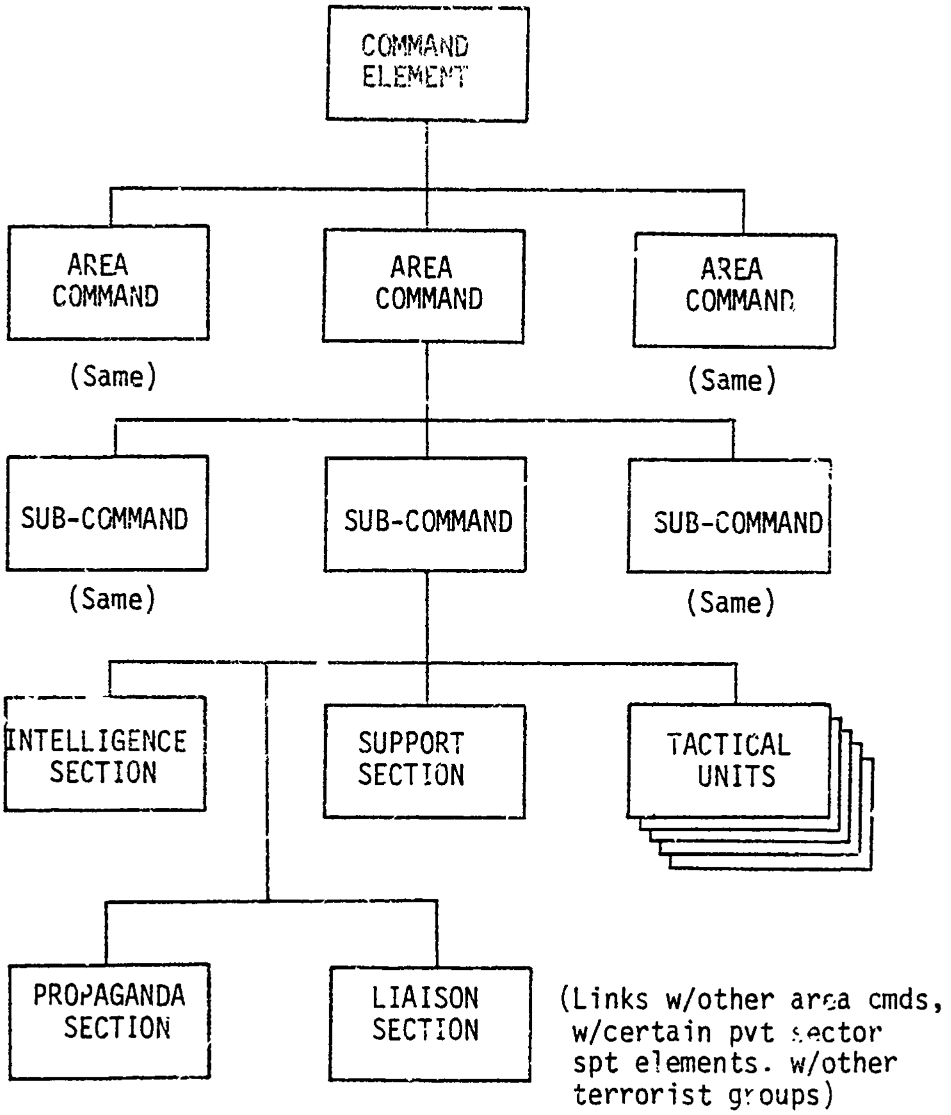


(Each unit has 2-3 cells of 2-5 persons each)

(typical medium-size terrorist group - more than 100, less than 500)



When groups grow with relative success and organizational effectiveness, which, as previously stated, is rarely possible, command elements organize subordinate area commands to maintain effective span of control over sub-commands, and sub-commands develop new sections to relieve tactical units and support sections of growing burdens. Example -



Structural variances among groups are not great. In Latin America, tactical units are called "firing groups", its cells "firing teams". Other groups use military terms, such as "platoon" and "squad". In all, the cell is the basic ingredient. Even the command element is composed of cells, in some groups so compartmentalized that one cell never works knowingly in concert with another....

3. Operations and "Patterns". There are seven (7) basic acts that modern terrorists (1968-present) have committed. In a hierarchy established by frequency of occurrences (most-repeated), these are -

- bombings
- hijackings/skyjackings
- kidnappings
- armed assaults/ambushes
- incendiary/arson
- assassinations
- hostage-taking/barricading

Following are total incidents,* by type, of these terrorist acts, 1968-1976.

ACT	TOTAL INCIDENTS
bombings	501
hijackings/skyjackings	146
kidnappings	137
armed assaults/ambushes	119
incendiary/arson	103

* excludes CONUS domestic/political acts

ACT	TOTAL INCIDENTS
assassinations	63
hostage-taking/barricading	35
other: 48	48
TOTAL	1,152

Almost one-third of these terrorist incidents 1968-1976 occurred in Western Europe. Following is a geographic outlay of these incidents:

AREA	TOTAL INCIDENTS
Western Europe	457
Latin America	327
Middle East	135
United States and Canada	146
Asia	54
Africa	12
USSR	22
Other	10
TOTAL	1,152

In 1968, there were 37 reported incidents, in 1976, 239, more than a 450 percent increase. The highest accumulation occurred in 1976 - 239 incidents. In 1974, there were 179. Below are annual totals -

YEAR	TOTAL INCIDENTS
1968	37
1969	55
1970	114
1971	63
1972	86

YEAR		TOTAL INCIDENTS
1973		211
1974		179
1975		168
1976		239
	TOTAL	1,152

Each year, except 1969 and 1970, bombings were the highest recorded incidents. In those two years, there were more than twice the skyjackings than bombings. The highest number of bombings occurred in 1974. There were 95.

During the 1968-76 period, most bombings occurred in Western Europe and the United States.

These are annual bombing incident rates, 1968-76:

YEAR		TOTAL BOMBINGS
1968		24
1969		17
1970		17
1971		15
1972		38
1973		81
1974		95
1975		88
1976		126
	TOTAL	501

Distributed geographically, these are -

AREA	TOTAL BOMBINGS/68-7
Western Europe	255
United States & Canada	81
Latin America	98
Middle East	46
Other: 19	21
TOTAL	501

Bombing incidents have ranged from the use of standard dynamite to sophisticated timed detonating devices with plastic explosives. They have been placed at airports, government buildings, commercial areas, and at Military installations. More than 90% of the terrorist acts against US Army and other DOD organizations have been bombings. In May, 1972, a bomb was placed in a stolen vehicle with stolen USAREUR plates. The vehicle was parked in the HQUSAREUR parking lot. The explosion killed three military personnel and damaged several buildings. In 1975, an Officers Club in Frankfurt, FRG, was bombed. An officer was killed, the club severely damaged. On 1 June, 1976, the same club was again bombed by terrorists, several injuries but no deaths the result. In December, 1976, a terrorist bomb exploded at the Rhine/Main AFB Officers Club, and in January, 1977, a POL storage tank at a US Army Post in Giessen. FRG, was also bombed.

Since 1968, terrorist bombings have caused around 125 casualties, more than twice the number caused by armed assaults. As stated earlier, bombings allow terrorists to act from afar - from geographical distance as well as time-distance — thus, a favorite tactic of the smaller group with minimum resources.

Terrorist hijacking/skyjackings took a sharp turn upward in 1969, 25 incidents against the 6 which occurred in 1968. In 1976, there were nine. Annual totals, 1968-76 were -

YEAR	TOTAL INCIDENTS
1968	6
1969	25
1970	47
1971	14
1972	16
1973	15
1974	9
1975	5
1976	9

It was in 1971 that efforts began internationally to curb skyjacking, resulting in airport security measures without which the incident rate may have remained as high, or gone higher than, the 1970 total. A single incident, however, can culminate in enormous damage. In 1970, PFLP terrorists blew up four hijacked high performance jet passenger aircraft outside Amman, Jordan, and Cairo, costing more than 100 million.

The greatest number of hijackings/skyjackings have originated in Latin America. Incidents, by area of origin, are -

AREA	TOTAL INCIDENTS
Latin America	44
U.S. and Canada	22
Western Europe	21
Middle East	21
USSR/Eastern Europe	15
Asia	17
Africa	6
TOTAL	146

Latin America terrorist groups also have the highest kidnapping rate, 87 between 1968-76. Africa follows with 17, Western Europe with 14. In the Middle East, there were 9, in the United States,and Canada, 3.

Worldwide, the highest annual kidnapping total was in 1973. There were 34. Following are annual totals.

YEAR	TOTAL INCIDENTS
1968	1
1969	3
1970	26
1971	10
1972	11
1973	34
1974	12
1975	26
1976	14
TOTAL	137

(Average length of victim captivity: 44 days)

In most cases, the kidnapped victim was a government or big business official. A US Army officer travelling in the Middle East was as a target of opportunity kidnapped and held hostage by a PFLP splinter group. In more than half the cases, ransom was included among demands set by perpetrators. In 1973, the ERP (Argentina) received about $60 million from Ford Motor Company for release of one of their executives.

Hostage-taking/Barricades have been greatest in Western Europe, the Munich Olympiad incident being the most well known. Of the 31 incidents during 1968-76 geographic distribution was -

AREA	TOTAL INCIDENTS
Western Europe	15
Middle East	9
Latin America	6

(Average length of hostages in captivity: 55 hours)

AREA	TOTAL INCIDENTS
Africa	9
Asia	2
US /Canada	1
TOTAL	35

Annual totals were -

YEAR	TOTAL INCIDENTS
1968	0
1969	0
1970	1
1971	1
1972	3
1973	8
1974	9
1975	9
1976	4
TOTAL	35

Western Europe experienced the greater number of armed assaults and ambushes during 1968-76. All were against government security forces or other persons representing authority. Geographic distribution was -

AREA	TOTAL INCIDENTS
Western Europe	37
Middle East	26
Latin America	28

AREA		TOTAL INCIDENTS
United States/Canada		10
Asia		9
Africa		6
	TOTAL	119

Armed assaults and ambushes during 1968-76 caused around 52 deaths and casualties. Annual incident rates were -

YEAR		TOTAL INCIDENTS
1968		2
1969		5
1970		6
1971		8
1972		6
1973		29
1974		24
1975		13
1976	TOTAL	119

Western Europe, during 1968-76, accrued the highest number of assassinations. Geographic distribution was -

AREA	TOTAL INCIDENTS
Western Europe	22
Latin America	23
Middle East	10
Asia	4

AREA		TOTAL INCIDENTS
United States/Canada		3
Africa		1
	TOTAL	63

Annually, totals were -

YEAR		TOTAL INCIDENTS
1968		4
1969		2
1970		6
1971		3
1972		4
1973		12
1974		8
1975		15
1976	TOTAL	63

Of the 59 incendiary/arson incidents, more than half took place in Western Europe. Geographic outlays show -

AREA	TOTAL INCIDENTS
Western Europe	67
Latin America	17
United States/Canada	10
Asia	7
Other	2
TOTAL	103

Most terrorist groups have repeatedly conducted more than two of the acts described. Some specialize more in one than another. The ERP and the Tupamaros were the first to perfect kidnapping. The PFLP has conducted many skyjackings. Below is a breakout of type acts and group perpetrations thereof -

a. Significant worst-case bombings (1968-76); 39 worst incidents involving total or near-total destruction, loss of life or severe casualties) -

(OCONUS)

GROUP	INCIDENTS
IRA	14
BSO	8
PFLP	5
Baader-Meinhof	5
Al Fatah	3
ERP	2
Tupamaros	1
"Carlos" Group	1

(CONUS)

GROUP	INCIDENTS
Deleted, AR 380-13	

b. Hijacking/Skyjacking (1968-76, 19 acts which resulted in damage, loss of life or physical harm and significant concessions).

(OCONUS)

GROUP	TOTAL INCIDENTS
PFLP	8
BSO	3
JRA	3
Al Fatah	2
ERP	2
Tupamaros	1

(CONUS) (no trend re. US terrorist groups and hijacking/skyjackings) (21 acts)

GROUP	TOTAL INCIDENTS
Deleted, AR 380-13	

c. Kidnappings (1968-76, 33 major incidents involving high officials and large ransoms)

(OCONUS)

GROUP	TOTAL INCIDENTS
Erritrean	11
ERP	11

GROUP	TOTAL INCIDENTS
Tupamaros	6
IRA	2
PFLP	2
BSO	1

(CCNUS) (no trend)

GROUP	TOTAL INCIDENTS
Deleted, AR 380-13	

d. Hostage-taking/Barricading (1968-76, 17 major incidents involving more than three hostages, significant concessions and lengthy government negotiations)

(OCONUS)

GROUP	TOTAL INCIDENTS
BSO	5
JRA	3
PFLP	2
"Carlos" Group	2
TOTAL	12

(CONUS) (no trend)

GROUP	TOTAL INCIDENTS
Deleted AR 380-13	

e. Armed Assaults and Ambushes (1968-76, 22 major incidents involving more than three adversaries and serious casualties or deaths)

(OCONUS)

GROUP	TOTAL INCIDENTS
BSO	7
Erritrean	6
PFLP	5
ERP	2
Tupamaros	1
JRA	1

(CONUS) (no trend) (Deleted AR 380-13)

f. Incendiary/Arson. Few groups have conducted major incendiary/arson incidents. OCONUS has witnessed two by the BSO and two by the PFLP, acts against facilities in Western Europe.

Trends evolve through analysis of the above-cited statistics. For example, in 1970 there were 47 hijackings/skyjackings, the highest recorded annually during 1968-76. The same year there were but 17 bombings and only one hostage-taking/barricade. Three years later, when international regulations prevented many hijackings/skyjackings, causing the rate to drop to 15, there were 81 bombings, 8 hostage-taking/barricades, and 34 kidnappings. Armed assaults and ambus[illegible] had also risen - from 6 in 1970 to 29 in 1973. In brief, a see-s[illegible] musical-chairs, effect seems to take place with selections from the terrorist operations inventory when one or more of the type acts are precluded by increased government activity. After awareness of terrorist kidnapping objectives, security measures on the part of potential victims caused the 1973 rate of 34 to drop to 12 in 1974. In 1974, there was a rise in hostage-taking and bombings. Thus, as direct actions by terrorists become more difficult to implement due to increased security or fear of overwhelming reprisals, indirect actions (such as bombings) increase. This occurred after the 1967 war when Palestinian terrorists were too weak to conduct active operations and resorted to letter-bombings, and when the IRA initiated bombing campaigns after British forces increased urban patrols.

Assassinations have been conducted by political and nationalistic groups, but not primarily to instill fear. Terrorist assassinations are often conducted to avenge harm, as in Black September's assassination of Jordan's Prime Minister in Cairo, 1971, or to eliminate specific blockages in a terrorist campaign, such as the murder of an effective police chief. Exceptions include the 1973 assassinations of Israeli officials by PFLP terrorists in Western Europe, and the 1975-76 "gunning" down of US officials in Greece, Cyprus and Iran.

Over the long term, the number of terrorist incidents conducted by a terrorist group may bring the most significant results. However, a single high-capacity incident can be more effective in achieving results than a dozen less violent. The BSO achieved more through a single hostage-taking/barricade act (the Munich massacre) than if they had conducted twenty bombings.

Peculiar, then, to the inventory of terrorist acts is the fact that the least conducted can have the greatest effect in terms of terrorist objectives, especially in bringing world attention to "cause". Even when perpetrators are killed in the process, dividends in publicity outweigh losses. There is no denying the BSO and PFLP hostage-taking/barricades of 1972 aided United Nations 1974 acceptance of the PLO.

A group that conducts the most operations is not always the most deadly. The "Carlos" Group, well known and feared, has conducted relatively few operations.

Below are tables describing (1) each group's total incidents, and (2) a ranking order based on number of grave, or more seriously damaging incidents.

Operations conducted by groups, 1968-76 -

(OCONUS) (167 major incidents)

GROUP	TOTAL
BSO (last act, 1974)	37
PFLP	27
ERP	23
Erritreans	23
IRA	17
Tupamaros *	12
JRA	8
Al Fatah	8
"Carlos" Group	7
Baader-Meinhof Remnants	6

* Weakened considerably by government counterterror forces.

(CONUS) (61 major incidents)

GROUP	TOTAL

Deleted, AR 380-13

g. Groups that have conducted the most flamboyant and repugnant terrorist acts, 1968-76 (acts which resulted in worldwide publicity, loss of lives, excessive monetary damage and costly counter-action).

(OCONUS) (23 incidents)

GROUP	TOTAL INCIDENTS
BSO	5
PFLP	5
JRA	2
"Carlos" Group	2
ERP	4
Tupamaros	3
IRA	2

(CONUS) (8 incidents)

GROUP	TOTAL INCIDENTS
Deleted, AR 380-13	

The more than 1,700 wounded and 800 deaths that resulted from 1968-76 incidents, when compared with casualties and deaths induced by war, seem insignificant. But in relation to total world violence, excluding war, in 1968 terrorism accounted for 18 percent of aggregate acts; in 1972, 48 percent; in 1975, 33 percent - large slices for a single type.

The frequency with which these acts occurred have exhibited some patterns. Many seem coincidental, and if not there has been no empirical data that through comparisons and analysis could provide 100% probabilities regarding the future of these patterns. As stated earlier, times and places of specific acts of terror remain somewhat unpredictable.

During 1969, an incident of terror occurred approximately every three months; in 1970, every two months; in 1971, except during the summer (June through August), when there were no incidents, every two months; in 1972, until September, every two months; and in 1973, except for April and October, every month. It was in December, 1973, that multiple incidents began to occur during a given month. A US Exxon oil executive was kidnapped by the ERP (Argentina), Spain's Premier was assassinated by the ETA (A Basque Separatist movement), and IRA bombings in London injured 60 persons. In 1974, there were two incidents receiving world attention every month through May, and more than four monthly June through December. In 1975, there were 2-3 similar incidents monthly. In December, 1975, four such incidents involved 22 continuous days of terror, more than 60 hostages, a kidnapped American, and the assassination of a US Embassy official. Thusly, incident patterns of the past two and one-half years show that on an average an act of terror receiving significant recognition occurs two to three times monthly. Since none of the groups perpetrating these acts have disbanded or weakened considerably, the trend may continue.

Other patterns emerge from the above when groups are viewed in relation to geopolitical rather than purely geographical circumstances. These are:

- Nationalist groups conduct more terror. Cuban exiles, activators of the least number of incidents among nationalistic groups, conducted nearly twice the incidents activated by the highest political or other type groups.

    - number of 1968-76 major incidents by nationalistic groups: 118
    - number of 1968-76 major incidents by other groups: 61

- Transnational/nationalistic groups conduct terror more violently and flamboyantly than others, choosing hijacking/skyjacking and hostage-taking/barricades over other type acts. Middle Eastern terrorists dominate this category.
- Domestic political groups seeking the overthrow of ruling governments conduct more kidnapping and armed assaults/ambushes.
- Domestic political groups rarely conduct hijackings/skyjackings.
- Religious groups conduct bombings more than any other act, and have conducted few hijackings/skyjackings or hostage-taking/barricades.
- Except for Spain, few incidents have been reported to have occurred in non-democratic countries where governments endorse repressive police measures.

Patterns are reflected seasonally -

- the most violent acts occurred between mid-May and mid-September...and when not in that period in a warm climatic area.

- Since 1973, December has been a month of high terror.

A general prognosis about terror can be obtained by matching the above derivations with the geopolitical circumstances surrounding terrorist groups. In western Europe, for example, the following geopolitical circumstances are bound to continue as characteristics of the operational environment of terrorist groups:

- West European governments, being democratic, do not impose repressive measures...such measures have spin-offs that restrict freedoms of innocent persons.
- Low, or minimum, popular support for terrorists...the economic and social values of western European countries satisfy most inhabitants.
- There are densely-populated urban centers, favoring covert tactics, security operations, communications, safe-houses, caches.
- There is a high concentration of varied targets, and wide-range 'media.'
- Most police and security forces are capable of effective counter-terror operations.
- There is a high number of USG personnel and facilities, and other Americans (proven terrorist targets).

Analysis of 1968-76 terrorist acts show that most take place where the above circumstances, or factors, exist in degrees favoring perpetrators.

Essentially, then, the following list of geopolitical circumstances/ factors are terror determinants which can be used to arrive at probabilities:

- incumbent politics/type restraints
- degree of popular support
- urban densitites
- availability of targets
- media
- effectiveness of police and other security forces
- number of USG facilities, personnel, other Americans.

Taking the above example, a less than 100% probability accuracy but obviously a more than educated guess/hunch probability can be made about Western Europe and terror. NOTE: The ambiguities of terror, and the variances among type groups and group objectives and capabilities, do not favor the equated 100% probability. Since 1970, scientists and analysts have worked data through all sorts of mathematical systems, to learn that feeding seven years of reported incidents into computers does not predict terror any better than astute observances of political and social change.

In balance, the above example shows that terror will continue in western Europe for some time, without sharp increase and no decline. Stable political values, effective police and security forces, and lack of popular support, will prevent terrorist groups from enlarging forces and increasing operations without igniting successful reprisals. Actions by the FRG against the Baader-Meinhof Gang corroborate this fact. Conversely, though, the unwillingness of Western Europe's democratic governments to initiate stringent security and investigative measures (because of repressive characteristics), plus high concentration of dense urban areas, wide-range media, availability of attractive targets, and the preponderance of USG facilities and US personnel, should continue to draw terrorists into action. The fulcrum, or balancing agent, that will keep terrorism at its present level or slightly higher in Western Europe will, of course, be the frequencies of operations that terrorist groups maintain. Sudden voluminous increases in terror would quickly upset the balance. For terrorists, whatever popular support does exist would dwindle, and police and other security measures would grow tenfold. Terror and counter-terror, unlike other forms of conflict resolution, are not restricted by rules of 'graduated response.'

Using the aame factors/method, probability statements about terror in other regions are possible. Data is easily obtained through US government area studies and historical accounts. Following are general probability summaries, by region:

(OCONUS)

(1) Western Europe

a. incumbent politics/type restraint:

- democratic procedures, allowing freedom of movement, passage, insecure targets, minimum restraint

b. Degree of popular support: low

c. Urban densities:

- numerous dense urban areas, allowing cells, safe-houses, communication, caches

d. Availability of targets:

- varied targets, such as airports, government buildings, engineering and energy facilities, embassies, military installations

e. Media: Maximum range, worldwide

f. Effectiveness of police and other security forces:

- high

g. Number of USG facilities, personnel, other Americans:

- US military - high
- US embassy officials - high
- US business - high
- US travellers - high
- US students - high

Prognosis: Political nuances, wide-range media, urban density, target availability, US facilities and personnel indicate that terror will continue in Western Europe. However, noted deterrences will prevent sharp increases.

(2) Latin America

a. Incumbent politics/type restraint:

- democratic but also militaristic, exercising maximum restraint in areas where government support is high

b. Degree of popular support:

- Argentina, high
- Uruguay, moderate
- other, low

c. Urban densities:

- numerous dense urban areas, allowing cells, safe-houses, communication, caches...

d. Availability of targets:

- high, and varied

e. Media: maximum range, cross-continent and in North America; re. US victims, worldwide

f. Effectiveness of police and other security forces:

- low in most countries, moderate to high in Argentina and Uruguay

g. USG facilities, personnel, other Americans:

- US military - moderate
- US embassy officials - high
- US business - moderate
- US travellers - moderate
- US students - low

Prognosis: Degree of popular support in certain areas, urban densities, availability of targets, media and less than very effective counter-terror forces, offset other factors, forming an indication that terror in Latin America may increase.

(3) Middle East

a. Incumbent politics/type restraint:

- Israel: democratic, but exercising maximum restraint/maximum reprisals
- Arab countries: democratic but also benevolent monarchial, exercising minimum restraint, yet maximum reprisals
- nuances discouraging internal terror, but encouraging external terror (transnational - outside middle east)

b. Degree of Popular Support:

- Israel: very low
- Arab countries: high, except Iran

c. Urban densities:

- moderate: Beirut, Tel Aviv, Jerusalem
- Israeli cities, effectively guarded

d. Availability of targets:

- high, varied, but guarded, especially in Israel

e. Media: low to moderate government intervention

f. Effectiveness of police and other security forces:

- Israel: high, very effective
- Arab countries: low to moderate

g. USG facilities, personnel, other Americans:

- US military - moderate
- US embassy officials - high

- US business - moderate, although high in Saudi Arabia, Iran, and Israel
- US travellers - low, but high in Israel
- US students - moderate

Prognosis:

- Israel: Political nuances, lack of popular support, media control, and effectiveness of counterterror forces, weigh against other factors. Unpredictable is the infrequent spectacular event, such as the 1972 LOD airport episode.

- Arab Countries: Arab incidents against Arabs are few. Fear of maximum reprisals (e.g., public hangings of three Palestinian terrorists, 1976) discourage frequent occurrences. Arab terror (BSO, PFLP, Al-Fatah) is transnational/nationalistic, more accurately predictable through analysis of other regions. Factored into a West European prognosis, Arab terror will continue. In the context of a Middle East prognosis, certain political nuances, such as increased inability for PLO terrorists to maintain support bases in Lebanon from which to launch actions into Israel, may force the PFLP, BSO, and Al-Fatah to plan more operations in Western Europe.

(CONUS)

a. Incumbent politics/type restraint

- democratic procedure allowing freedom of movement, passage, insecure targets, minimum restraint

b. Degree of popular support: low

c. Urban densities

- numerous dense urban areas, allowing ce.ls, safe-houses, communication, caches.

d. Availability of targets

- high, and varied

e. Media: maximum range, worldwide

f. Effectiveness of police and other security forces:

- high during terror and post-terror activities...prohibited by law during pre-terror periods from conducting active investigations without probable cause ..

g. Government and foreign government personnel:

- Federal, state, local: high
- Military - moderate
- Foreign government - moderate in Washington, D.C., and New York City
- Foreign military - low

Prognosis: The low degree of popular support for terror, and effective police and other security forces at various governmental levels, neutralize advant ges in other factors. Political nuances and urban densities make it possible for terrorist groups to form, move about, hide, but difficult to conduct operations without extreme post-operational pressure. Terror, in

CONUS, is likely to continue with newly-formed groups and infrequent attempts by existing ones. However, should performance and technology among US terrorist groups improve, the infrequent attempts could be devastating, as in CONUS exists the greater abundance of attractive targets - more airports, nuclear reactors, military installations, isolated government buildings, hydro-electric and communication facilities, cross-continent computer systems. Transnational groups based outside CONUS that want increased credibility and world attention cannot but eye the American cornucopia of targets with great hunger.

Summarily, then, the outlays and probabilities described above imply that terror will continue in OCONUS and CONUS unless dramatic changes occur among the political, social and other variables presented, with slight increases due to situational factors effecting transnational/nationalistic terrorists at regional and national levels, (e.g., the PFLP, BSO, and Lebanon) and because of increased cooperation among major terrorist groups for operational purposes.

4. Modus Operandi (Terrorist Tactics, 1977/83 Terrorist Group Profile)

Terrorist groups conduct operations in small bands comprising 8-12 trained personnel carrying light automatic weapons, hand grenades, basic explosives, and transistor radios to remain aware of public reactions to their acts or to hear pre-arranged codes broadcast by stations in supporting countries. They dress similar to indigenous persons and carry light rations and ammunition for several days. Teams include an assault element and a security element, with leaders serving as negotiators. During hostage-taking/barricades, kidnappings, and hijackings/skyjackings, personnel of both elements take turns at 'security' that is, guarding victims, and observing entrances and exits to target areas and watching counter-terror forces. Like infantry defending in built-up areas, they maintain fields of fire and keep weapons loaded and ready. When possible, more than one terrorist guards an entrance or exit simultaneously, changing exact postions frequently. Hostages are usually separated to prevent their communicating or planning escape and from intelligence-gathering. To preclude such intelligence, terrorists talk in front of their victims in code other languages and with code-names. Unless provoking, hostages and other victims are rarely harmed.

Pre-operational activities by terrorist groups include meticulous planning, reconnaissance missions, and lengthy periods of training and rehearsals. Plans are conceived and prepared by command elements. Target and area reconnaissance missions are conducted by special units (intelligence sections) or by one-time agents who have target and area access. It is rare when planners, reconnaissance teams or agents, and actual perpetrators know each other or meet. Information is passed up and down through intermediaries (cut-outs/liaison sections). Training and rehearsals take place in countries outside the target area, with perpetrators, even leaders, having no knowledge of what their specific target will be until it is time to move to conduct the operation.

Movement to targets is covert, perpetrators departing individually or in pairs along separate and often circuitous routes, when necessary with fake passports and false names.

Weapons and other items travel separately, reaching pre-arranged sites near targets where they are given to perpetrators sometimes moments before the terrorist act. Supporting countries have allowed diplomatic pouches as carriers for these items, agents taking them from embassies to pre-arranged sites. In many cases, these agents have been members of cooperating terrorist groups. More than twelve cases have been reported where weapons have been sent through diplomatic pouch by Cuba to terrorists in Western Europe and Latin America. Baader-Meinhof terrorists (FRG) and members of Italy's Red Brigade assisted in the delivery of weapons used by the BSO during the Munich Massacre.

More than 300 Latin American terrorists have received training in subversion, weaponry, infiltration and negotiating practices from Cuba, and more than 100 terrorists in Western Europe and the Middle East have been trained in the Soviet Union, North Korea, Algeria, Libya, and Northern Ireland. Japanese and West European terrorists have received training from Palestinian forces in Lebanon. These terrorists are of above-average intelligence, between ages 23-30, speak more than one language, often English, are excellent marksmen, adapt readily to changes in operational environments, and seem to be effective at disappearing into "undergrounds" and assuming "new covers".

Direct terrorist operations (e.g., hostage-taking/barricades, hijackings/skyjackings, kidnapping and assaults/ambushes), include the following sequential phases:

- movement to target
- infiltration
- assault
- occupation
- demands and negotiations (continuous)
- safe departure or escape; or:
- violent defense until captured, casualty-ridden or killed.

Following are characteristics among groups during these phases:

- <u>movement to target</u>
    - covert
    - indigenous dress
    - fake identification/covers
    - individual, or in pairs
    - circuitous routes
    - no equipment
    - only leader or one more of terrorists may have specific knowledge of target
- <u>infiltration</u>
    - terrorists assemble at pre-arranged site or safe-house
    - covert
    - indigenous dress
    - precision and control
    - speed
    - weapons under cover
    - communications
    - possible use of on-site agents, or accompanying agents

- assault
  - precision and control
  - speed and surprise
  - visible weapons
  - communications
  - individual and small unit tactics
  - security
  - collection of hostages
  - exploitation of fear and uncertainty among hostages
- occupation
  - security
  - assignments of responsibility
  - care and control of hostages
  - selection of, or confirmation of, escape routes...escape planning
  - communications
  - protection and placement of equipment and supplies
  - care and feeding
- demands and negotiations
  - pronouncements by chief negotiator or leader
  - display of terrorist credibility
  - receipt of response from counter-terror officials
  - terrorist assessment of response
  - terrorist assessment of opposing tactical forces
  - bargaining, but much unwillingness to compromise

- safe departure or escape; or defense
  - intense security
  - use of hostages (infrequent during safe departure)
  - visible weapons (violent use during defense)
  - vulnerable to effective well-planted snipers
  - night operations
  - communications

Once an operation is launched, terrorists act in relation to opposition. Few groups enter into operations without contingency plans. Groups have been known to infiltrate and assault alternate targets. Several aircraft belonging to one airline were hijacked when the initially selected aircraft of another were found by terrorists to be too heavily guarded. Alternate demands have been negotiated frequently, and some groups have been known to have several departure and escape plans.

Except for advances in attainment of weapons, analyses show that the above-described profile will probably not change much beyond 1983-1990.

5. Targets

Repeated material targets of terrorist operations have been civil aviation (aircraft hijackings/skyjackings), embassies (hostage-taking/barricading), buildings and other facilities symbolizing government authority, and military installations or sites. In the Middle East, Palestinian terrorists have assaulted school buses, schools, apartment-houses and hotels. In Latin America and Northern Ireland, attacks on military installations have been greater.

Human targets have been embassy and other government officials, corporation executives, military officials, police, dependents of VIPs, Considering the broad spectrum of targets available to terrorists, the inventory to date seems narrow. One reason for this is the sensitivity among terrorists to total alienation from their cause on the part of a general body-politic. Confining operations and targets to symbols of government authority rather than targets connected in some way to social values limits the alienation process. Even so, US government and other officials and analysts agree that in the near future terrorists will increase the target inventory. Type targets expected are -

- engineering and energy systems, such as:
  - hydro-electric plants
  - off-shore oil rigs
  - nuclear facilities/sites
  - water reservoirs*
  - gas pipelines
  - dams*
  - electric power lines
- communication lines and facilities
- increased military installations/sites
- private sector locations catering to military personnel
- chemical storage sites
- shipyards and dock facilities
- equipment warehouses
- rail-lines/rail-cars
- bus depots
- trucks/truck facilities

* Unique in volume to U.S. Army Corps of Engineers/Civil Works.

- management information systems (computerized)

Analysts cite new potential human targets being -

- dependents of embassy and other government officials
- dependents of military officials
- foreign professionals (engineers, scientists)
- innocent travellers

While US Army Corps of Engineer Civil Works projects have a high target attraction value, they also have a low security profile. This is not to mean that these projects are surrounded by lack of security concern; rather, the nature and locations of these projects, which are not on military installations, increase their exposure as targets and decrease the capability of law enforcement organizations to secure projects adequately against potential terrorism. For example, few, if any, of these Civil Works projects have sufficient attendant security personnel to counter vandalism, assaults, or sabotage attempts, let alone a terrorist attack to seize and barricade hostages.

The field operating agencies of the Corps of Engineers must rely on non-organic assets, or upon agreements with local civilian police or, in some cases, upon contract personnel, for security and to respond to incidents; dedicated security operations assets are unavailable to the Corps of Engineers.

The impact of the Corps of Engineers' unique security problem is obviously worthy of inclusion in an extension of current US Army study to identify potential terrorist targets the vulnerability factors of these targets, and the appropriate approach to developing countermeasures to reduce their vulnerability to terrorist acts.

Because of a lack of precedents, predicting volumes and frequencies of the above as future targets is difficult. It is their availability and their attractiveness that makes one believe terrorists will attempt them. Also, as current repeated targets become difficult to approach due to improved blankets of security, terrorists seek the new and different. Selection of some of the listed future potential targets, in this view, seems inevitable. In some areas, where there does not exist sufficient political or social turmoil for terrorists to justify attacks against government buildings or officials (such as the United States) issues more likely to engender less anti-terrorist behavior might determine target selections; for example, local environmental issues serving as catalysts toward terrorist destruction of off-shore oil rigs, nuclear facilities and other energy systems.

At present, the Director of Civil Works for the US Army Corps of Engineers is responsible for more than 4,000 separate projects, which include design, construction, maintenance and operation of "works" for navigation, flood control, hydro-electric power production, water supply, water quality and flow control, and beach and shore protection. The budget authorizations for these activities approximate $42 billion.

Nuclear/Chemical. Certainly the "nuclear" facility or site, whether civilian or military, causes much fear and concern as a potential terrorist target. The damage to life and property, the immense monetary, political and other concessions that can be "extorted" through nuclear targets, are sufficient reasons to thicken and surround them with effective security, irrespective of the results of probability studies.

Recent US and international legal breakthroughs, combined with growing needs for new energy, have provided for a proliferation of new nuclear facilities, namely reactors. Several studies reflect that within 10 years, 30 more countries may have nuclear weapons and/or reactors. This alone widens the spectrum of potential nuclear targets considerably.

Of significant nuclear incidents reported since 1970, there have been hoaxes, attempted radioactive contaminations, a dismantling, an incendiary attack, an overt threat (demorstrated by the appearance of explosives on-site), and hostage-taking barricades.

None of these incidents resulted in severe damage, death or physical harm. Three of the incidents were attributed to major terroris-groups, Baader-Meinhof and the ERP.

To date, major terrorist groups have displayed little interest in concentrating on acts against nuclear installations. But if terrorists choose to destroy aircraft in flight and kill 73 innocent passengers (Cubana Airlines, 6 October 1976), to assume limited nuclear action on their part is not unrealistic.

A study delivered to the California Seminar on Arms Control and Foreign Policy*, October, 1975, listed type potential nuclear terrorist acts as -

- A nuclear hoax (claiming to have materials to set off a nuclear explosion unless demands are met).
- Limited, or low-level, sabotage of a nuclear facility.

* RAND Corporation, Brian Jenkins, October 1975.

- Seizure of a nuclear installation, or a portion thereof (hostage-taking/barricade).
- Theft of a weapon, components, or plutonium.
- Radioactive contamination.
- Detonation of nuclear devices in unpopulated remote areas (as a show of force).
- Deliberate dispersal of plutonium or other toxic radioactive materials.
- Detonation of a stolen or homemade nuclear bomb in a populated area (the most extreme scenario).

Analyses of terrorist incidents between 1968-1976 show that major terrorist organizations match operational risks and post-operational goals with the consequences that terrorist acts can deliver. That is, most terrorist groups do not invest in acts of terror when returns (legitimate countermeasures) can seriously jeopardize their future capabilities or cause goal-oriented setbacks. Soviet and East European reactions to acts of terror show that the greater the consequences (government countermeasures), the greater the decrease in potential terror. Thus, analysis of the consequences that the above-listed nuclear terror acts would promulgate for terrorist groups could provide reliable assumptions about one-time or repeated occurrences of the acts. Of the eight possible nuclear terror acts listed above, in sequence from least harmful to most devastating, each implies obvious consequences, or legitimate government countermeasures that would impact adversely, in intensifying degrees up the ladder of type acts, against terrorists and their goals. For example, a terrorist attempt to disperse plutonium among a population may give license to government officials to exert extreme pressure in tracking down terrorists and enacting laws and security measures that would make it practically impossible for terrorists to act again, while low-level sabotage or seizure of an installation without resulting harm to any person could actually enhance popular support, especially among environmentalists, and prevent serious countermeasures. This factor, coupled with analyses of existing terrorist goals and their capabilities to withstand post-operational pressure, points out that terrorist groups operating now and near-future would select the first three acts listed rather than risk consequences that would evolve through use of the remaining, escalating five. Further, mass contamination or destruction through nuclear means, as opposed to the threat of such actions, in no way connects to known or projected limited or ultimate terrorist objectives, except in the case of the mentally disturbed. Concern about the overall terrorist threat to nuclear installations should concentrate, heavily, then, upon possibilities of hoaxes, low-level sabotage, seizure (hostage-taking/barricades), limited contamination and theft, and less upon detonation and destruction, although the latter must by no means be ignored.

That terror is theatre, designed to spread fear and uncertainty, is an added factor implying that terrorists will seek nuclear targets. Other targets repeatedly used evenually lose dramatic appeal. Terrorists must then find other targets that will rejuvenate the continuing terror story, just as dramatists add the unusual to enlarge viewing audiences of soap-operas. Nuclear targets rate high among "attention-getters". Further, terrorist groups more than once suffered operational defeat to such degrees they selected to quickly conduct operations of great violence so as to regain credibility. The PFLP/JRA coordinated attack at LOD airport in 1972, was such an act, following a previous attempt that failed. No doubt, successful nuclear terror could serve this purpose.

Chemical terror is another form with far-reaching potential effects. In comparison with nuclear terror. it is difficult to determine which could be worse. Some relief exists, however, in the fact that there are methods to reduce the effects of chemical terror whereas not as much can be done about the effects of nuclear explosions. Against chemical agents, people can wear protective masks, inject combative serums, wear certain cloting, take medicines. Unless used in great quantities (endangering terrorists as well as victims and target-audiences) destruction is nowhere quickly as complete as nuclear. But the drama, and ensuing panic, would compare with that created by nuclear threat or use, as people are as repulsed, perhaps moreso, by use of chemical agents and illnesses, paralysis and deaths occurring therefrom.

Potential terrorist acts against chemical storage sites are similar to those for nuclear, including hoaxes, sabotage, contaminations, seizure (hostage-taking/barricades), theft, and limited or maximum use of agents. Additionally, the same factors applying to terrorist decisions to select nuclear targets apply to the chemical. Variances exist as follows:

- Although extremely difficult, it would be easier to obtain chemical agents (via black market or through supporting nations) than nuclear devices, and
- it would be easier to manufacture certain lethal agents with obtainable raw elements; further
- it would be easier for terrorists to conceal chemical agents once stolen than to do same with most nuclear items.

Terrorist groups, then, should:

- continue to select targets used in the pəst
- increase selection of certain type targets when preferred targets become less accessible
- widen the inventory of targets to include energy and engineering-environmental systems
- increase selection of U.S. military targets
- select nuclear and chemical targets, infrequently, to conduct limited terror (less than mass destruction) under the following conditions:

  - need exists on part of terrorists to rejuvenate overall dramatic impact and credibility of terror
  - need exists on part of terrorists to regain organizational credibility (vengeance reaction)
  - terrorist assessments of other type acts prove only nuclear or chemical terror could serve to obtain objectives, i.e., payoffs to terrorist demands

USG Facilities, personnel, other Americans. In August, 1976 three American employess of a US firm were killed by terrorists in Iran. Since 1968, more than 59 Americans have been kidnap victims, and 136 US installations were bombed. The total number of transnational/international incidents involving US citizens and property in this period includes -

Act	US Targets (Citizens & Property)	Other	Total	% US
Bombings	166	335	501	33%
Kidnappings	64	73	137	46%
Assaults/Ambushes	40	79	119	33%
Incendiaries	45	58	103	43%
Hijackings/skyjackings	30	116	146	20%
Assassinations	22	41	63	34%
Hostage-taking/Barricades	5	30	35	14%
Other	19	39	48	3%
TOTAL	391	761	1,152	33%

Of the total international/transnational terrorist acts that occurred in 1968 (37), 5 involved US citizens and property, around 13.5 percent. In 1975, of 168, 47 involved Americans, approximately 28 percent, more than twice the 1968 slice. Although 1973 witnessed the highest number of acts against US citizens/property (85 out of 211 acts) in 1970 and 1971 more than half the incidents, each year, were against US citizens/property. Shown are acts involving Americans, compared with acts against others.

Year	U.S. Targets	Other	Total	Percentage, U.S.
1968	5	32	37	13.5%
1969	16	39	55	29%
1970	56	58	114	49%
1971	38	25	63	60%
1972	26	60	86	30%
1973	85	126	211	40%
1974	57	122	179	32%
1975	47	121	168	28%
1976	61	178	239	25%
TOTALS	391	761	1,152	33%

Breakouts, by type act, are -

(Bombings)

Year	U.S. Targets	Other	Total	Percentage, U.S.
1968	1	23	24	4%
1969	9	8	17	53%
1970	12	5	17	71%
1971	12	3	15	80%
1972	18	20	38	47%
1973	34	47	81	42%
1974	32	63	95	34%
1975	18	70	88	20%
1976	30	96	126	23%

(Kidnappings)

Year	U.S. Targets	Other	Total	Percentage, U.S.
1968	1	0	1	100%
1969	2	1	3	67%
1970	15	11	26	58%
1971	4	6	10	40%
1972	1	10	11	9%
1973	18	16	34	53%
1974	5	7	12	42%
1975	13	13	26	50%
1976	5	9	14	35%

(Assaults/Ambushes)

Year	U.S. Targets	Other	Total	Percentage, U.S.
1968	0	2	2	0
1969	1	4	5	20%
1970	4	2	6	80%
1971	4	4	8	50%
1972	2	4	6	33%
1973	14	15	29	48%
1974	6	18	24	25%
1975	6	9	15	40%
1976	3	21	24	12%

(Incendiaries)

Year	U.S. Targets	Other	Total	Percentage, U.S.
1968	0	0	0	0%
1969	1	1	2	50%
1970	1	1	2	50%
1971	5	1	6	83%
1972	1	2	3	33%
1973	12	8	20	60%
1974	7	4	11	64%
1975	6	9	15	40%
1976	12	32	44	27%

(hijacking/skyjackings)

Year	U.S. Targets	Other	Total	Percentage, U.S.
1968	0	6	6	0
1969	1	24	25	4%
1970	16	31	47	34%
1971	7	7	14	50%
1972	3	13	16	19%
1973	0	15	15	0
1974	2	7	9	22%
1975	0	5	5	0
1976	1	8	9	11%

(assassinations)

Year	U.S. Targets	Other	Total	Percentage, U.S.
1968	3	1	4	75%
1969	1	1	2	50%
1970	3	3	6	50%
1971	0	3	3	0
1972	0	4	4	0
1973	3	9	12	25%
1974	2	6	8	25%
1975	3	6	9	33%
1976	7	8	15	53%

(hostage-taking/barricades)

Year	U.S. Targets	Other	Total	Percentage, U.S.
1968	0	0	0	0
1969	0	0	0	0
1970	0	1	1	0
1971	0	1	1	0
1972	0	3	3	0
1973	2	6	8	25%
1974	1	8	9	11%
1975	1	8	9	11%
1976	1	3	4	25%

In summary -

- Except for 1968 and 1975, the majority of all bombings were of U.S.-related targets.
- Since 1973, kidnappings of U.S. personnel were approximately half that of other victims.
- Except for 1970, U.S.-related targets in assaults/ ambushes were 50 percent or less of annual totals.
- Except for 1972 and 1975, U.S. incendiary targets were half or more than others.
- US-related hijackings/skyjackings were less than 35 percent each year.
- Except for 1968-70, U.S. assassination targets accounted for 33 percent or less each year.
- The highest number of U.S. citizens assassinated in any year was three (3).
- Hostage-taking/barricades of U.S. citizens/property in any year was 25 percent or less.
- Excluding 1968, over 40 percent of total targets were U.S.-related...as high as 60 percent in 1971.
- Bombings of U.S. targets have each year been greater in number than other acts against U.S. targets
- Hostage-taking/barricades and hijackings/skyjackings are conducted least by terrorists against U.S. citizens/ property

With respect to assassinations, of 68 between 1968-75, 4 were U.S. diplomats and one an Army Attache assigned to a U.S. Embassy. In kidnappings, 9 of 59 U.S. personnel were diplomats. Most of the remaining were DoD and private corporation officials.

U.S. citizens and property hold high symbolic values among terrorists. U.S. targets result in the widest exploitation of media, the largest kidnapping ransoms (to date, Argentine terrorists have amassed more than $60 million from U.S. corporations), and the greatest potential pressure, or influence, upon target audiences. Because of America's economic, military and technological position in the world, these values are likely to remain high among terrorists, the above-cited targetting patterns staying in force.

Total Targets.

An analysis of how international/transnational terrorist incidents increased (or decreased) from year to year, follows:

Year	Total Incidents	Annual % Increases/Decreases
1968	37	base-year
1969	55	48% (increase over 1968)
1970	114	107% (over 1969)
1971	63	-45% (from 1970)
1972	86	37% (over 1971)
1973	211	145% (over 1972)
1974	179	-15% (from 1973)
1975	168	-6% (from 1974)
1976	239	41% (from 1975)

Although incidents dropped considerably in 1971, increases in 1970 and 1973 raised the 1968-76 total sharply. The percentage increase, 1968 compared with 1976, is 454 percent. That is, against 1968, terrorist incidents have quadrupled.

The decreases in incidents in 1974 and 1975 were slight. By the end of 1976 - a year that witnessed some severe terrorist acts (Entebbe; bombings of U.S. Officers Clubs, Frankfurt/Rhein Main; assassinations of U.S. firm employees, Iran; explosion of Cubana Airline, killing 73 persons; more than 100 bombings, incendiaries and harrassments following suicide of Ulrike Meinhof), an increase in total incidents was reflected. Statistically, a three year 1974-1976 base would show that total terrorist acts might continue at around the 1974 level (179 incidents per year).

V. DoD and US Army Installations, 1968-1975

From 1968 through 1975, there were around 111 terrorist acts against Dod installations, sites, personnel, equipment. Between 1946 and 1968, only 7 incidents occurred, and there were none between 1947 and 1957; nor from 1959 through 1963, nor 1965 through 1967. Yet, in those years nearly 500 acts were conducted by terrorists against other targets. Balancing a 21 year span (1946-1967) against a subsequent 8-year span, the marked difference appears as -

1946-1967:	7 acts
1968-1975:	111 acts

During period one (1946-1967), excluding Korea and Vietnam, a greater percentage of DoD and US Army personnel existed in areas where terrorists operated than during period two (1968-1975). Terrorists at that time (period one) concentrated on obtaining concessions/limited objectives from their target audiences directly, rarely through intermediary victims. That is, a close relationship between victim and target existed. In period two, acts against DoD targets increased around the same time the world witnessed an emergence of transnational/nationalistic terrorists in Western Europe and international/political urban terrorists in Latin America. In 1971, a year high in incidents perpetrated by these type groups, the highest number of acts against Dod - 33 - occurred, accounting for almost half the total acts and nearly all of those against US targets. It appears, then, attacks on Dod targets rises with the increase in transnational and international groups.

During 1975, more than 17 percent of total terrorist incidents were against DoD targets, accounting for over half of the acts against US targets. Because of obvious disparity between acts conducted in periods one and two, above, reflecting that intents (motives) more specific than that DoD targets may have been more physically accessible than others, a conclusion that DoD targets are selected by terrorists for strategic reasons is quite valid. Couched in political, social and military terms, the following list includes reasons why terrorist groups target, and would continue to target, DoD military and/or civilian personnel and/or property.

DoD targets -

- symbolize
  - capitalist theory
  - "instruments of imperialism"
  - establishment authority
  - wealth
  - advanced technology
  - preponderance of resources
  - third-party influence in host-countries
  - military power
- include nuclear facilities/sites
- attract "media" worldwide
- include specific military targets
- include energy and engineering - environmental systems/Civil Works
- Include potential for terrorist acquisition of arms and equipment (via theft)
- might bring huge ransoms

- in several cases relate to specific political, social or environmental issues
- could serve as intermediary victim to coerce U.S. government into exercising international influence (i.e., U.S. Army installation as victim, USG-foreign policy as target)
- could serve as dummy-antagonist in terrorist campaign to divide a population and create dissent (i.e., U.S. as scapegoat to mobilize popular support)
- could serve in vengeance operations to protest U.S. policy or previous U.S. measures against terror or a specific terrorist group
- could serve to establish or re-establish a terrorist group's ability to attack desirable targets in spectacular fashion

Immediate, or limited, tactical terrorist objectives in attacking DoD targets, have been, or would be to -

- create immediate anti-military feelings within the surrounding population
- cause U.S. military forces to over-react, reinforcing the above
- demonstrate weakness of U.S. security forces and or of host-country forces
- harrass U.S. military personnel, instill fear, undermine morale
- create slow-downs in project development (e.g., U.S. Army Corps of Engineer projects)

- prevent development of new installations, facilities, sites that might enhance U.S. position favorably
- destroy installations, facilities, sites, for reasons directly above
- cause relocations
- embarrass military officials
- embarrass host-country officials
- depress local economy
- confine DoD and U.S. Army personnel to specific areas
- prevent exploitation of nuclear technology (peaceful-energy producing...or defense-oriented)
- prevent U.S. Army from achieving training objectives
- test credibility of U.S. security procedures
- demand release of prisoners

Other reasons -

- as surrogates, attacking for another terrorist group
- security may be lax and targets have easy access
- targets are accessible because of agents within (i.e., the man inside, U.S. or, as in OCONUS, the indigenous)

As stated, in years 1968-1975, there were around 111 terrorist acts against DoD installations. Following is the year-by-year breakout.

Year	Incidents
1968	2
1969	1
1970	30
1971	33

Year	Incidents
1972	6
1973	13
1974	7
1975	28

(total-111)

By the end of 1971, the increase was over one-thousand percent. The lowest number of incidents that occurred since 1970 (6 in 1972) is but one less than the total incidents which occurred 1946 through 1968, and is 200 percent greater than the highest annual number of incidents against DoD targets of the period.

Geographically, acts between 1968-75 against DoD were -

Region	Incidents
Western Europe	42
Middle East	13
Latin America	8
Asia	5
Africa	2
Near East (Turkey)	5
CONUS	36

(total-111)

The 1975 total - 28 - represents the widest geographical spread, as shown -

Country	Incidents
Greece	6
Turkey	5
Japan	3
Iran	2
Argentina	1

Country	Incidents
Beirut	1
Guatemala	1
Ethiopia	1
Kuala Lumpur	1
Italy	1
Spain	1
CONUS	5

(total-28)

The 1975 total also showed wide use among type acts. Shown -

Type Act	Incidents
Incendiaries	11
Bombings	7
Kidnappings	4 (1 unsuccessful attempt)
Hostage-taking/ Barricading	1
Assassination	1
Assault/Ambushes	1
Other (harrassment)	1

(total-28)

Extracting 1975 acts against U.S. Army targets shows 9 incidents as -

Type Act	Incidents
Bombings	3
Kidnappings	3 (1 unsuccessful)
Hostage-taking/ Barricading	1
Incendiary	1
Other (harrassment)	1

(total-9)

In 1975, total terrorist acts against all type targets, U.S.-related and others, was 168.

Cf 1975 total US transnational and international incidents (47), US Army targets alone accounted for 17 percent.

Developments, then, from the above data are -

- Most incidents against DoD targets occur in Western Europe and CONUS, and next Middle East
- Incendiaries and bombings are higher among DoD targets
- To "extort", kidnappings of DoD and US Army personnel are selected above hostage-taking/barricades, which would be more difficult on guarded installations.
- DoD targets are high among US-related, and US Army high among DoD.

DoD targets represent values inherent in structures that terrorists view as "the opposition". If today's number of terrorist groups remain or increase slightly, and political, social, environmental and military factors also remain as is, acts against DoD personnel/property are likely to continue at a fluctuating level of 20-30 incidents per year. And when it becomes increasingly difficult for terrorists to act against other US targets (e.g., embassies) it is likely they may increase acts against DoD. In CONUS, in the sixties, US terrorists attempted to establish metropolitan police as targets symbolizing repressive government. The attempt failed. A group including some of these terrorists in 1975 conducted a bombing at US Army Installation, Fort Ord. One incident is no proof of intent; however, as seen by terrorists it would be practical to shift from the policeman to the soldier, who is no more revered, if a new symbolic target for terror is perceived necessary.

VI. Equipment and Technology

To date, terrorists and terrorist groups have rarely used other than basic arms during operations - normally rifles and light automatic weapons, hand grenades and simple explosives. These have included -

- U.S. M-1's
- U.S. M-16's
- U.S. Carbines (M-1 and M-2)
- Kalishnikovs (AK-47's)
- Bren Machine Guns (Great Britain)
- Warsaw Pact rifles and SMG's
- Chinese carbines
- Sniper-scopes
- Soviet and U.S-made fragmentation hand-grenades
- Miniature detonating devices (as in letter-bombs)
- Dynamite
- C-4
- Napalm
- Molotov cocktails

A terrorist incident involving advanced weaponry occurred outside Rome Airport (Italy) where Arab terrorists were armed with a Russian "Strella" (SA-7). This Soviet weapon, like America's "Redeye", is a shoulder-fired, anti-aircraft, heat-seeking missile using an infrared homing device. The incident occurred in 1973. Certainly, advanced weaponry is within the reach of terrorist groups Leading supporters, such as Libya's Quaddafi, could easily be persuaded to obtain non-nuclear man-portable weapons of the more sophisticated genre for several terrorist operations. As listed in a recent study*, present and near-future attractive weapons of this range might be -

- a Belgian silent mortar weighing but 22 pounds
- the "Dragon", a U.S. wire-guided anti-tank missile around 30 pounds, operable by one person
- the "Blowpipe", a British surface-to-surface and surface-to-air man-portable missile
- The RB-70, a Swedish surface-to-air missile weighing around 170 pounds, conveniently breakable into components so as to be carried by several persons in small packages
- the U.S. "Stinger", similar to "Redeye", with improved velocity
- the "Milan", a West German (FRG) one-man portable guidance missile system
- the FRG "Armbrust 300", an anti-tank weapon without backblast, ideal for urban terror
- U.S. M-79 grenade-launchers with advanced projectiles capable of going through several inches of steel plate and igniting fuel

* High Technology Terrorism and Surrogate War, Brian Jenkins, California, 1975

- Miniature mines
- M-60 machine-guns

Factors encouraging terrorists to use advanced weaponry are -

- necessary to destroy specific targets
- greater accuracy and faster killing power during assaults/ambushes and defensive shootouts
- dramatic effect, attracting media worldwide
- facilitates creating fear
- easier to transport and conceal
- establish or regain image of power or credibility
- facilitates security (i.e., aids protection during infiltrations and escapes)
- substitutes for direct action (as mortars, or bombs, to be used indirectly)

Factors discouraging terrorists from using advanced weaponry would be:

- escalation of opposition capability (development of better forces, hardening of targets, increased weapons support)
- effects may cause reprisals, or escalations of conflict, that terrorists could not defend against (creating setbacks re. terrorists' ultimate goals)
- effects may cause terrorist popular support, or chances for such, to deteriorate
- some items may be too cumbersome, hindering transport and concealment as well as individual tactics
- new and complex training may be required
- small parts (components) may be difficult to replace
- expensive acquisition and storage (monetarily)
- "one-shot fired" capability

Whether terrorists will use advanced weaponry or not regularly will depend on their willingness to risk maximum consequences relative to their associated acts. Considering current ultimate goals of today's terrorist groups, their capabilities, degrees of popular support, and the potential reactions of most legitimate government security forces it does not seem that there will be rearmaments of terrorists with the type weapons described above on grand sharply-increasing scales. However, the following does seem probable -

- As inventories of advanced weaponry increase, so does availability. Terrorists will find access to such weapons easier. If nothing else, temptations to test advanced weapons will cause several uses.

- Technology in any form is subject to progress. What is used currently turns over and becomes obsolete. Terrorists who once used M-1 rifles now use M-16's. Some rapid-firing weapon more effective and deadly will replace the M-16 and eventually fall into the hands of terrorists.

- The weapon with a "bigger bang" would certainly eliminate any developing casual ho-hum attitudes about terrorism after long runs of small operations using basic arms. To prevent the loss of "drama" in terrorism, advanced weaponry would play an important role.

Briefly, it appears that -

- terrorists operating today will use advanced weaponry which will not hinder future operational capability, risk popular support, or cause goal-oriented setbacks.

- these terrorists will use advanced weaponry that has high risk potential infrequently - to achieve dramatic effect, destroy specific targets, establish or regain power or credibility.

- the natural flow of progress and its distribution spin-off could eventually place highly-advanced non-nuclear weapons into the hands of terrorists...this flow and emplacement would be gradual over a period of several years.

VI. Conclusion

Terror is aggravating world order as frequently and intensely, with similar damaging results, as period 1974 through 1976. Acts against the U.S. Army have increased. Now and near-future, the U.S. Army can expect terrorist acts by individuals, individual domestic or transnational groups, and by cooperating domestic or transnational groups. Acts by international terrorists, developed for surrogate warfare by nations whose interests conflict with those of the USG, are less probable.

BIBLIOGRAPHY

Books

1. Burton, Anthony M. Urban Terrorism: Theory, Practice and Response. London: Cooper, 1975.

2. Clutterbuck, Richard L. Protest and the Urban Guerrilla. New York: Abelard-Schuman, 1974.

3. Dobson, Christopher. Black September. New York: Macmillan, 1974.

4. Kennedy, G. The Military and the Third World. New York: Scribner's, 1974.

5. Moss, Robert. The War for the Cities. New York: Coward, McCann and Geoghegan, 1972.

6. O'Ballance, Edgar. Arab Guerrilla Warfare. London, 1964.

Studies

1. Annual of Power and Conflict, 1973-1974. London: Institute for the Study of Conflict, 1974...Same: 1974-1975.

2. Extremist Groups in the United States. Vestermark, S.D. International Association of Chiefs of Police, 1975.

3. European Theatre Terrorist Groups. Goodman, Hoffman, McClanahan, Tompkins, USAF. Air University, 1976.

4. Fatality of Illusions: Dominant Images of International Terrorism. Wilkinson, Paul. Presented at U.S. Dept. of State-sponsored conference on International Terrorism, Washington, D. C., 1976.

5. File on Arab Terrorism. Yaholm, Dan Jerusalem: Carta Publications, 1973.

6. High Technology Terrorism and Surrogate War: The Impact of New Technology on Low-Level Violence. Jenkins, Brian. Rand Corporation, 1975.

7. Hostage Survival: Some Preliminary Observations. Jenkins, Brian. 1976.

8. Insurgent Terrorism and its Use by the Viet Cong. La Charite, Norman. Washington, D. C. Center for Research in Social Systems, American University, 1969.

9. International Terrorism: A Chronology, 1968-1974. Jenkins, Brian and Johnson, Janera. Rand Corporation, 1975.

10. Numbered Lives: Some Statistical Observations from 77 International Hostage Episodes. Jenkins, Johnson, Ronfeldt. Rand Corporation, 1975.

11. On International Terrorism: Historical and Contemporary Aspects (1968-1975). Bouthoul, G. French Institute of Polemology. Presented at U.S. Dept of State-sponsored Conference on International Terrorism, Washington, D. C., 1976.

12. Research Study, International and Transnational Terrorism: Diagnosis and Prognosis. Central Intelligence Agency, April, 1976 (Unclassified).

13. Terrorism: A Staff Study. Committee on Internal Security, U.S. House of Representatives, 93d Congress, 1974.

14. Terrorism: The Problem in Perspective. Crozier, Brian. Presented at U.S. Dept of State-sponsored Conference on International Terrorism, Washington, D. C. 1976.

15. Threat Analysis Methodology. Reber, J.R. International Association of Chiefs of Police, 1976.

16. Threat Assessment-Civil Aviation. US Federal Aviation Administration, 1976.

17. Will Terrorists Go Nuclear? Jenkins, Brian. Discussion Paper No. 64, California Seminar on Arms Control and Foreign Policy, 1975.

18. World Terror: The Palestine Liberation Organization (PLO). Leibstone, Marvin. Presented OACSI, U.S. Army, 1975.

Articles and Periodicals

1 Action and Reaction: West Germany and the Baader-Meinhof Guerrillas. Elliott, John D. Strategic Review, Winter, 1976.

2. American Companies Act Against Terrorism in Iran, Washington, Post, 22 November 1976.

3. Biological Warfare and the Urban Battleground, Griffith, G.W. Enforcement Journal. Vol. 14, 1975.

4. Cuban Extremists in US: A Growing Terror Threat, US News and World Report, 6 December, 1976.

5. Croatian Terrorists, Washington Post, 14 September 1976.

6. Diplomats Slain Past Eight Years, NY Times, 17 June 1976.

7. Excerpts from "Prairie Fire", Political Statement of the Weather Underground, Skeptic, Fall, 1974.

8. FBI Says Bombings on Rise, New Terrorist Units Forming, Security Systems Digest, 3 December 1975.

9. Major Terrorist Bands, NY Times, 23 July 1976.

10. Nuclear Terrorism and the Escalation of International Conflict. Frank, Forrest R., Naval War College Review, Fall 1976

11. Rightist Terror Stirs Argentina, NY Times, 29 August 1976.

12. Skyjackings: Bombs for Croatia, Time, 20 September, 1976.

13. Syria Vows Revenge for Embassy Attacks. Washington Star, 12 October 1976.

14. Terrorists: Exit Carlos, NEWSWEEK, 27 September, 1976.

15. Terrorist Gangs: Who They Are, What They've Done, US News and World Report, 5 January 1976.

16. Terrorist Techniques Improve, and So Do Efforts to Block Them, NY Times, 23 July 1976.

17. The Failure of Terrorism. Laquer, Walter. Harper's Magazine, March, 1976.

18. The Man Known as Carlos, TIME, 5 January, 1976.

19. Three US Civilians Slain...in Teheran, NY Times, 29 August, 1976.

20. The Strategy of Terrorism. Fromkin, David. Foreign Affairs, July, 1975.

21. Undergrounds and the Uses of Terror. Leibstone, Marvin. Military Intelligence Magazine, Summer-Fall, 1975.

22. Weather Underground has "Blue-print for Terror". Koziol, R. Chicago Tribune, 14 March, 1976.

23. West Germany and a Disciple of Despair (Ulrike Meinhof), TIME, 24 May, 1976

24. Will "Hot Pursuit" Stop Terrorism? US News and World Report, 19 July 1976.

25. World Terrorists and Chemical Warfare, Albany Times-Union, New York. Page 1, 28 November 1976.

Terrorist Literature

1. Minimanual of the Irish Guerrilla. Ireland

2. Minimanual of the Urban Guerrilla. Marighella, Carlos. Brazil.

3. On Organizing Urban Guerrilla Units. Anonymous, codenamed Field Marshall, District of Columbia.

4. Philosophy of the Urban Gurerrilia. Guillen, Abraham.

5. Selected Writings, Mao Tse Tung.

APPENDIX B

CRISIS MANAGEMENT
FOR
TERRORISM
AND OTHER
MAJOR DISRUPTIONS ON
U.S. ARMY INSTALLATIONS

CRISIS MANAGEMENT FOR TERRORISM ON U.S. ARMY INSTALLATIONS

I. GENERAL

U.S. Army installations do not all have the same vulnerability to terrorist acts or incidents. Vulnerability depends on many factors. Actions can be taken that will deter, or assist in preventing, terrorist acts or incidents. Predicting a terrorist group's intentions. with any degree of accuracy, is dependent upon accurate intelligence. With the highly restrictive policies concerning intelligence gathering activities and the filing and retention of information, a capability to forecast or predict terrorists intentions (with any accuracy) does not exist. Even if this were possible terrorist acts would not be positively prevented. Merely, the probability for success would go down while the risk for the terrorist would go up. Without adequate intelligence there will be little leadtime, if any, leaving little specific forewarning of a terrorist attack or other disruptive activity. There must be a predetermined plan for managing the crisis created by a terrorist attack and the plan must be able to be put into effect as expeditiously as possible.

Due to the political overtones of most terrorist acts, reaction to the situation can involve the military and U.S. Government at every level - from the responsible individual at the scene to the President in the White House. There must be complete coordination for the U.S. to react with solidarity. Certain decisions will be made at a high level while others made at intermediate and lower levels. This requires a crisis management structure, delineating command and control and flow of information. A steady flow of accurate information is an absolute necessity. Since terrorism is basically criminal activity with political or diplomatic overtones some general areas of responsibilities and guidelines have been established.

- The Department of Justice is the primary agency in coping with terrorism in the 50 states, the Commonwealth of Puerto Rico, and U.S. possessions and territories. Investigative and operational responsibility rest with the Federal Bureau of Investigation.

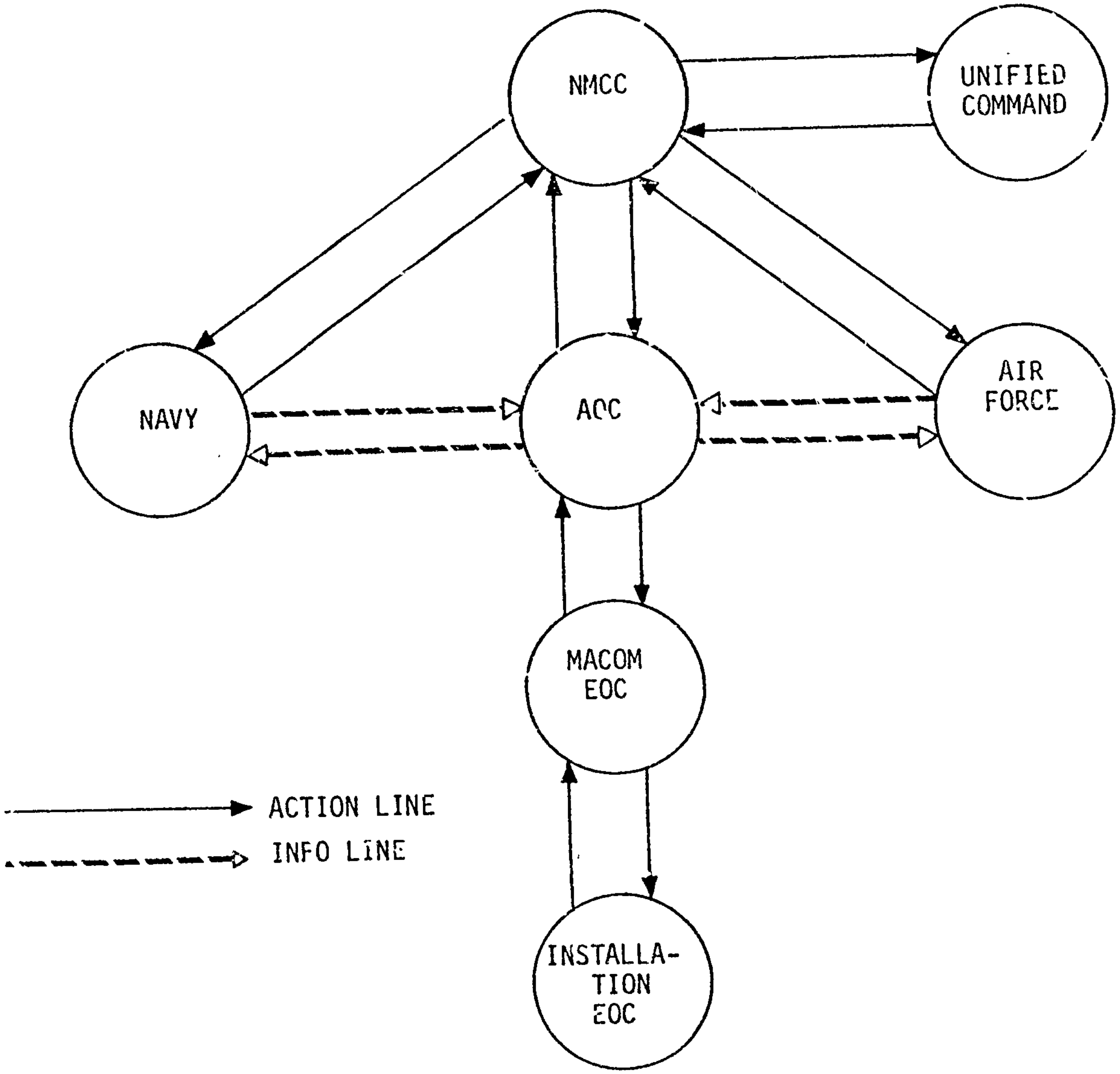
- The Department of State has the primary responsibility for dealing with terrorism involving Americans abroad, which includes the military, and for handling foreign relations aspects of U.S. domestic terrorist incidents.

- Actual command and operational control of U.S. military forces will remain with the U.S. military.

II. REPORTING AND TRANSITION TO CRISIS MANAGEMENT STRUCTURE

In order to cope with any type of crisis management situation there must be in existence a basic operational type of active communications network. This communications network does exist as shown in Figure 1. The National Military Command Center (NMCC) acts not only as the command post for the Joint Chiefs of Staff but also for the Secretary of Defense. It can be considered the command post for the Department of Defense. The NMCC maintains active communications with the Unified Commands, over which the Secretary of Defense maintains operational control, as well as the operations centers of the three Military Departments. The Army Operations Center (AOC) is capable of lateral communications with the Navy and Air Force. On a routine basis the AOC is manned 24 hours a day monitoring and passing routine traffic to and from the NMCC and the major army commands (MACOM). The MACOM maintain what is generally called an Emergency Operations Center (EOC). The EOC serves the same purpose for the MACOM as does the AOC for HQ Department of the Army. At installation level there are varying forms of EOC. These are sometimes maintained in a standby or "caretaker" status. At every Army installation there should be an area designated as an EOC with standby communications ready to be activated for 24 hour operation should a major

FIGURE 1. ROUTINE COMMUNICATIONS



disruption occur on the installation. This basic network forms the nucleus for an expanded crisis management command and control structure.

The initial report of a terrorist act against an Army installation could have many origins. It may be the threat of an act, such as a bomb threat, sent to the news media who in turn would place it on the wire services. It may originate through civil authorities or federal authorities, such as the FBI. The most probable origin of the report for an impending terrorist crisis will be at the targeted installation. No matter what the origin the report must reach the AOC immediately. The existing Serious Incident Reporting procedures establisned by AR 190-40 provides such a system. This reporting system provides an alert to HQ DA that a terrorist incident (defined as a Category I incident being of immediate concern to DA or DOD) has occurred, or may occur. In the case of terrorist acts even a credible threat should be reported as a Category I incident. If there is any doubt the decision must be made in favor of making the report. In the case of terrorism directed against Army installations the highest military and civilian leaders must receive early notification. Additionally, when the Serious Incident Report of terrorism is made in Army channels the report must be submitted to the FBI (in the case of installations in the 50 states, U.S. territories or possessions) or the unified command (in the case of overseas installations). Once the report is received by any of the elements shown on Figure 1 it should be immediately relayed to the otner elements indicated by the arrows. This alerts the primary elements throughout the DOD of the terrorist incident, or the threat of such an incident.

When the report of a terrorist incident is received by the AOC the on duty team chief will refer to a "terrorism" emergency action card. This emergency action card, similar to other AOC emergency action cards, shall contain step by step instructions to be taken immediately when the initial report is received, to include specific notifications.

A policy statement delineating terrorism as a crime, and coping with terrorism a law enforcement function, should be issued. The DCSPER (DAPE-HRE) should be designated, in writing, as the DA staff element responsible for coping with terrorism and providing the DA terrorist crisis manager.

Once the initial report of a terrorist incident on an Army installation is received at the AOC and the initial notifications have been made, a decision must be reached concerning augmentation of the AOC. The following represents a complete augmentation which constitutes the HQ DA terrorism crisis management team. This team must be capable of sustained operations. It consists of pre-designated on-call representatives from the DA Staff elements indicated below. Procedures for accomplishing the foregoing should be spelled out in DA Memo 1-4.

- ODCSPER General Officer - This individual acts as the overall manager of the crisis management team melding together the various disciplines represented.

- ODCSPER-Law Enforcement - This individual acts as the principal advisor to the ODCSPER General Officer. He must be familiar with law enforcement capabilities and policies that would affect the decision making process concerning the terrorist crisis at hand.

- ODCSOPS/Military Support - This individual provides expertise in providing military support to non-Army agencies and activities.

- ODCSOPS/Current Operations - This individual provides expertise on the geographic area in which the terrorist incident has occurred.

- ODCSOPS/Communications and Electronics - This individual provides advice and assistance in assuring adequate and reliable communications throughout the crisis management structure. He must be able to pinpoint additional communications assets that may be required. He also works with the Military Support team member in providing required communications to support non-Army agencies, such as the FBI.

- ODCSLOG/Explosive Ordnance Disposal - This individual provides advice on all matters related to render safe and disposal of explosive devices and munitions. He would be oarticularly valuable in terrorist bomb threat situations.

- ODCSLOG/Transportation - This individual maintains status and availability of transportation assets that may be required, both in support of the Army activities involved in the situation, as well as non-Army agencies.

- OACSI - This individual is in addition to the normal OACSI element in the AOC. He is responsible for analyzing intelligence reports from agencies and activities external to the Army as well as directing the Army Military Intelligence support in handling the crisis.

- USACIDC - This individual is responsible for analyzing criminal reports from agencies and activities external to the Army, as well as directing the USACIDC support in handling the crisis.

- Public Affairs - This individual must provide assistance in preparing and making announcement to the news media and the public in general. He must be fully cognizant of DOD and other Governmental Agency policies regarding news releases relative to terrorist incidents. He should maintain a file of releases already made at all levels. It is critical that all announcements at all levels are consistent with one another.

- Office of the Surgeon General - This individual should primarily provide advice in the discipline of psychology, particularly useful in hostage situations. While not able to directly apply psychological techniques to the situation he can collaborate with, or advise his colleagues involved in the crisis situation. He should also be able to obtain non-Army sources of such expertise, if required.

- Office of the Judge Advocate General - This individual serves as the legal member of the crisis management team. Questions of a legal nature should be anticipated during the terrorism crisis. Of particular importance would be questions of jurisc.ction and legality of any decision on concessions to demands.

- Department of Justice/FBI Representative - For a terrorist crisis occurring on an Army installation located within the 50 states, U.S. territories or possessions this individual provides a valuable service to the team since the FBI normally has jurisdiction in these cases. This representation, along with installed communications in the AOC augmentation room, is already provided for in Civil Disturbance (Garden Plot) AOC augmentation. It provides for an invaluable liaison with the responsible Federal Agency.

- Briefing Team - Many questions and updates will be required during a terrorism crisis situation. The team members should not be diverted from their primary team functions to prepare and participate in briefings on the situation. .he team members should merely provide input to the briefing team. The briefing team continuously maintains a current situation briefing along with necessary visual aids.

While the foregoing represents a complete crisis management team, which should be able to manage the most severe terrorist crisis, a partial augmentation using only selected expertise may be more appropriate - depending on information contained in the initial report. Establishment of a crisis management team at the installation EOC should match the same disciplines as the DA crisis management team, with some obvious exceptions. The installation crisis management team will no doubt be smaller with some individuals providing expertise in more than one area. In any event, the installation crisis management team must be pre-designated by name and exercised periodically, to assure that contingency plans to cope with major disruptions are current and effective.

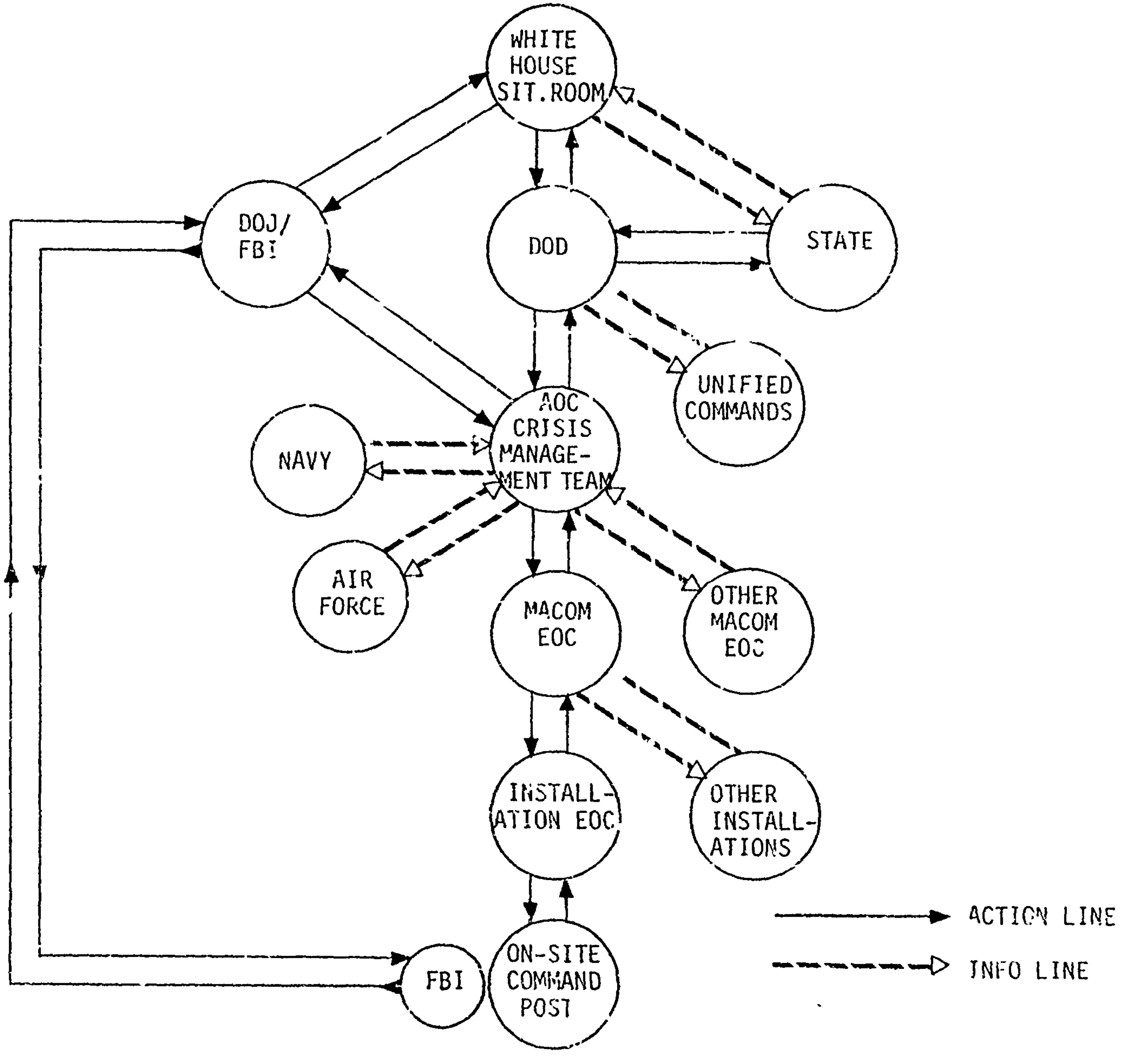
III. TERRORIST CRISIS 50 U.S. STATES, TERRITORIES, AND POSSESSIONS

As previously mentioned, investigative and operational responsibility for most terrorist acts occurring within the 50 U.S. states, territories, and possessions (including the Panama Canal Zone) rests with the Federal Bureau of Investigation under the Department of Justice. For a terrorist act occurring on an Army installation geographically located within the FBI jurisdictional boundaries Army resources will normally be provided the FBI agent in charge if required. At the same time the actual command and operational control of Army forces remains with the Army. Control of the situation pending arrival of the FBI will be an installation responsibility. Pre-established agreements should spell out precisely the role of the FBI subsequent to their arrival at the scene. All of this considered collectively creates a need for a chain of command. A "top to bottom" communications network and pre-determined control center relationships must be established with minimum delay. This network is shown at Figure 2.

The first element that receives a report of terrorism makes an initial internal notification while at the same time notifying other elements as indicated by the arrows. The information is passed to those elements indicated by the broken lines. This insures that all levels are aware of an actual or threatened terrorist act. Each one of the elements has a role in the crisis management network.

- Army Operations Center (AOC) - Upon receiving a report of a terrorist incident the AOC Team Chief should immediately notify the DA Staff point of contact indicated on the emergency action card. Then notification should be made to the NMCC and the FBI. If the report did not originate with the MACOM or installation, then they should be alerted. Other MACOM should be informed of the situation, as well as the Navy and Air Force. In the meantime the DA Staff point of contact recommends and obtains a decision as to AOC augmentation, either partial or full, in accordance with applicable internal staff procedures. Dedicated communications circuits are established for the crisis management team direct to the FBI, the NMCC, through the MACOM EOC to the affected installation EOC. These communications links are indicated by the solid lines at Figure 2. The primary function of the DA crisis management team is to establish centralized control for actions by the U.S. Army in response to, or in support of, successful neutralization of the incident. This provides the installation a single command and control line for military actions.

FIGURE 2. TERRORIST CRISIS 50 U.S. STATES, TERRITORIES, POSSESSIONS



- Department of Justice/Federal Bureau of Investigation - As previously stated the DOJ/FBI has overall U.S. Government responsibility for coping with terrorist acts occurring on U.S. territory. Upon notification of a terrorist act on a U.S. Army installation dedicated communications would be established as indicated at Figure 2. While not shown on Figure 2, it is anticipated that the FBI would establish a communications link with the State Department, that has responsibility for international political implications of terrorism. All U.S. Army support requirements would be relayed to the AOC as well as information concerning instructions being issued to the FBI agent(s) at the scene. It is anticipated that there would be a continuous dialogue between DOJ/FBI and the AOC crisis management team. Additionally, DOJ/FBI would be the logical element in the crisis management structure to keep the White House situation room informed and any Presidential decisions would be relayed to DOJ,FBI to be carried out.

- Department of Defense (DOD) - The Office of the Assistant Secretary of Defense (International Security Affairs) serves as the focal point for terrorism within the Office of the Secretary of Defense. It is this focal point that provides the interface for the DOD with the Department of State. For terrorist incidents occurring in the U.S. the Special Assistant to the Secretary of Defense and the Deputy Secretary of Defense will be part of the DOD Ad Hoc Task Force, as is the case involving civil disturbance problems. The National Military Command Center may provide the facility for the DOD Ad Hoc Task Force.

- State Department - As previously mentioned, the State Department is the U.S. Government lead agency for the international political implications of terrorism. In the case of terrorism occurring within U.S. jurisdictional boundaries the State Department would closely monitor the situation for the international implications that may arise. The State Department would also be involved in the decision process where any political implications to major demands would be considered. Additionally, the State Department would provide information concerning international implications to the White House situation room.

- Major Army Command Emergency Operations Center (MACOM EOC) - While the MACOM EOC normally would function as a command post, the extreme sensitivity of terrorism to national interests and the need for possible highly centralized control, communications must be established from the AOC to the targeted installation, through the MACOM EOC. This prevents delay and possible misunderstandings of communications. The MACOM EOC will, however, monitor these communications between the AOC and the targeted installation to stay abreast of the situation as well as keep other installations in the command informed, as deemed necessary. This serves as an alert to possible widespread terrorism within the command.

- Installation Emergency Operations Center (IEOC) - As mentioned previously in Section II the installation crisis management team should, for the most part, match the disciplines represented by the DA crisis management team at the AOC. One additional source of information may be required, that of the facilities engineer who would provide building floor plans, utility diagrams, etc. to be used in coping with a hostage barricade situation. Depending on local agreements, representation from civil authorities may be provided for at the IEOC. The installation IEOC serves as a buffer, or filter, to the individual in charge at the scene. It may be more desirable to have the FBI communications terminate at the IEOC, provided the agent-in-charge agreed. This type of decision would depend on the situation and would be made by prior mutual agreement between the senior FBI official and the installation commander. Specific operations and tactics at the scene, to include the functioning of the on-site command post, are covered in Field Counter-Terror Operations, Appendix C.

IV. TERRORIST CRISIS U.S. INSTALLATION IN FOREIGN COUNTRY

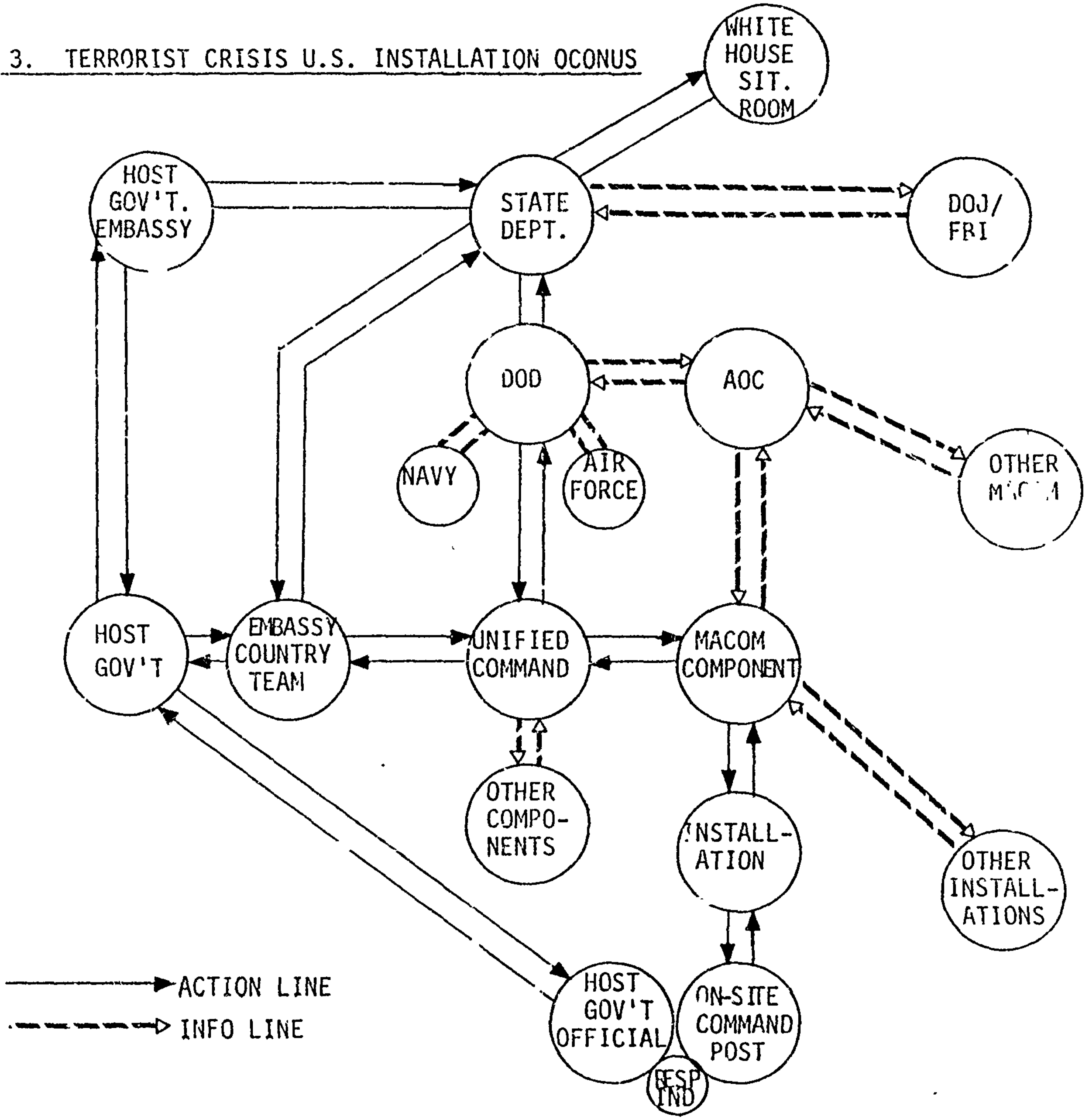
The Department of State has responsibility for developing the U.S. Government response to terrorist acts that have significant diplomatic or political ramifications on U.S. installations in overseas areas. In the case of terrorism on U.S. installations in foreign countries the crisis management structure becomes complex, primarily due to the overriding international implications and jurisdiction. The other major factor is the difference in the U.S. military command structure where the major army command is a component of a unified command reporting to the Secretary of Defense and the Joint Chiefs of Staff. The initial report, in this case, will most likely originate from the overseas command with the NMCC and the AOC being jointly notified.

When a terrorist act or incident occurs on a U.S. Army installation overseas a pre-determined communications and control network must be established with minimum delay. Command and control relationships must be understood. Such a network is shown at Figure 3. Each one of the elements shown in the Figure has a role in the crisis management network.

- Army Operations Center (AOC) - When a terrorist act occurs on a U.S. Army installation overseas the crisis management becomes extremely complex; however, the role of the AOC is primarily one of monitoring the situation and the military chain of command is from the Secretary of Defense to the unified command. The AOC should receive current information from OSD and the operations center of the unified command army component; e.g., USAREUR. The AOC would alert other Army major commands to the situations, primarily for informational purposes. In this situation a complete augmentation of the AOC, in all probability, would not be required.

- Department of Defense (DOD) - In the event of a terrorist crisis on a military installation OCONUS a DOD Ad Hoc Task Force would be established. This task force would probably be chaired by a representative of the Office of the Assistant Secretary of Defense (International Security Affairs) with representation from the Joint Staff and the involved Military Department. The National Military Command Center can provide the facility from which the Ad Hoc Task Force could operate, and, in any event should serve as the communications center for OSD during a terrorist crisis. If the crisis is one of primarily military involvement, without diplomatic or political ramifications, the DOD

FIGURE 3. TERRORIST CRISIS U.S. INSTALLATION OCONUS



would provide overall management of the situation with the Department of State serving in an advisory capacity. On the other hand, if the situation does involve diplomatic or political ramifications the Department of State assumes overall management with the Ad Hoc Task Force managing the DOD support. The NMCC should provide current information to the AOC, which in this case assumes a monitoring and support role.

- Unified Command - The operations center at the overseas unified command serves as the "in-country" extension of the NMCC. It provides the operations command post whereby operational control of the U.S. Army component is exercised in peacetime. During a terrorist crisis situation the unified command also would serve as the military point of contact with the U.S. Embassy. The unified command should also inform the other component commands of the terrorist crisis and issue appropriate increased alert instructions. The unified command should be the only element which issues operational instructions to the component command/Army major command.

- Army Component Command/Major Army Command - The component command of the unified command (e.g., USAREUR) receives operational control and direction from the unified command(e.g., USEUCOM). The severity of the crisis would dictate the degree of operations center augmentation required. The component command should also notify other installations to the situation and issue necessary instructions for increased alert, as deemed necessary. Additionally, the Army Operations Center should be kept fully informed since this link could serve as an alternate chain of command should communications through the unified command to the NMCC be disrupted.

- Installation Emergency Operations Center (IEOC) - The IEOC in an overseas area performs essentially the same function as the IEOC in the U.S. described previously in Section III; however, it is anticipated that some host nation representation will be present. This would, of course, depend on existing local agreements. The IEOC is the element where immediate decisions will be made and is just one "generation" removed from the scene of the crisis. Specific operations and tactics at the scene, to include the functions of the on-site command post, are covered in Field Counter-Terror Operations, Appendix C.

- State Department - if a terrorist act or incident generates political or diplomatic ramifications, the Department of State assumes responsibility for and management of the U.S. Government response. This agency will provide overall policy and direction to the DOD Ad Hoc Task Force. It is anticipated that close liaison will be maintained with the host country embassy in Washington, D. C. as well as keeping the White House Situation Room informed of the crisis. The State Department will, in all probability, maintain continuous communications with the U.S. Embassy in the country where the terrorist act has occurred.

- Host Government Embassy, Washington, D. C. - The host government will probably stay in close contact with the State Department in order to insure close coordination of effort in neutralizing the crisis, particularly if major jurisdictional problems should arise that must be resolved at the highest levels. The host government embassy would also pass information back to the host country government.

- Host Country Government - The host country plays varying degrees of importance, depending on the country involved and applicable international agreements in effect - particularly Status of Forces Agreements. It should be anticipated that direct communications with Department of State may be desired, which would depend on the sensitivity and severity of the crisis. Also, the host country government will, in all probability, establish lines of communication to host country officials at the scene of the crisis. There would be direct communications with the U.S. Embassy in the host country, because the U.S. Ambassador is responsible for all Americans in the country.

- U.S. Embassy - The U.S. Embassy, in the name of the Ambassador, acts as the highest U.S. authority within the country. During a terrorist crisis the country team would be ideally suited to serve as a crisis management team for the Ambassador. The U.S. Embassy would be in close communication with the host government, U.S. Department of State, and the unified command.

APPENDIX C

MILITARY INSTALLATION
FIELD COUNTER-TERROR
OPERATIONS:

ORGANIZATIONAL AND TACTICAL MODELS

FIELD COUNTER-TERROR OPERATIONS

I. INTRODUCTION

a. Scope and Method. This section deals with method, skills and techniques for use on site during U.S. Army operations to counter terrorism on military installations. Although the scope of probabilities for terrorist acts on installations or sites comprises incidents which could cause the use of combat task forces, Ranger units, or Special Forces detachments, it is more likely near future and 1983 acts against the U.S. Army, in a majority of cases, will require but local U.S. Army law enforcement personnel. Thus, this section focuses primarily on actions to be met by these personnel.

Included for consideration is a package of inter-related field countermeasures that, driven by policy and under the supervision of installation commanders, can, in response to terror, be implemented on-site, by in-being installation command and staff, Provost Marshals, law enforcement Special Reaction Forces and appropriate support elements.

The countermeasures presented evolved from a design created by the SAI study team against base line data secured during an analysis of the terrorist threat, and through event tree analysis which insured an appropriate list of options for research toward recommended measures. The design, clearly basic, was deliberately trimmed to test available U.S. Army assets and resources cost effectively, meeting the problems of response head on without leaving gaps. The design - essentially a list of operational task areas - begins with a critical time related start point - the moment of recognition that a terrorist incident has occurred on a military installation. The end point of the design includes post event measures - those acts which should be considered for use after the freeing of hostages, capture of terrorists, or other climactic points.

In sequence, the study design comprised the following:

- Crisis-management
  - Opns center
  - Fwd cmd post
    - Command and control/chain of command
    - Staffing/skill requirements
    - Procedures/Tasks
    - Location
    - Equipment
    - Communications
- Problems of Jurisdiction
  - Military
  - Federal, state, local
  - Foreign (Host Country)
- Response
  - Organization(S)
    - Combat arms/combat support
      - fixed assets
      - task forcing
    - Law enforcement
      - fixed assets
      - Special Reaction Force/Teams
        - duties and responsibilities
        - alert levels
        - mobilization procedures
        - movement to operational areas

- security
- communications
- equipment
- negotiating
- hostage protection
- use of special weapons and devices
- individual and team tactics, to include assaults
- capturing terrorists
- liaison with media and with federal, state and local officials.

Reactions to terrorism occur in one of three phases: pre-event, event, and post event. The material in this section is concerned with the latter two, event and post event, that is, with theories and practices of response - more precisely, situational control and tactics.

b. Force Characteristics. The principal actors in this segment of the study are terrorist organizations as defined in the 1977/1983 terrorist group profile, Appendix A, Threat Analysis, and U.S. Army combat, combat support and specifically law enforcement personnel as they exist under present TOE's. Cautiously, the countermeasures that are presented for consideration were developed as reactions that are pursuant to the capabilities of above mentioned U.S. Army personnel in opposition to the cited terrorist group profiles. To arrive at countermeasures, actions by one force were pitted against another, of course in hypothetical situations (via simulation).

c. Terrorist Situations. To achieve countermeasure options for field operations, a set of terrorist acts on military installations was staged (simulated) and prioritized, then re-staged (simulated). Standards for selection were based on an examination of probable terrorist group objectives for conducting operations against the U.S. Army, and by determining the type operation best suited for attainment of these objectives. For example, if a terrorist group's objective is to attain worldwide publicity and to embarrass U.S. military forces it might select to enter a headquarters/office building on a supposedly secure installation. barricade and hold hostages, thereby achieving media attention and stalemating military forces, rather than conduct bombings or thefts, which would not bring in the publicity or possible humiliation desired. Conversely, if an objective is to create fear and limited harrassment or disruption, bombings would seem an appropriate tactic. Appendix A, includes a full range of probable terrorist group objectives toward the U.S. Army and the most likely operations they (that is, the proposed 1977/1983 groups) would select to attain them. These operations, or incidents, represent the terrorist situations the following countermeasures can challenge effectively.

II. CRISIS MANAGEMENT

a. Operational Constraints. There are several considerations distinguishing most terrorist situations (hypothesized as taking place on military installations) from other criminal acts, and these need be taken into account when designing measures to deal with them. These are:

- The outcome of a terrorist act can impact beyond military installations and affect, adversely, U.S. domestic and foreign policy.

- Innocent persons, in addition to military personnel, can be harmed more severely than in most like criminal acts and are in greater danger of being killed.

- Terrorist and/or U.S. Army actions in a terror/counter-terror situation can easily be misinterpreted by media with unnecessary harm ensuing.

- Sensitive and expensive resources may be involved, causing disruptions at high governmental levels.

It is because of these constraints that countermeasures must be forged from processes that factor in a greater number of variables than might be studied when designing ways to respond to crimes that are similar to terrorist acts but which do not have the same far reaching effects. The social and political consequences of a response to terror, as stated, must be weighed in balance with military consequences to ascertain cost/risk developments prior to selection of countermeasures for enactment. Therefore, decisions to commit counterterror forces for tactical operations should be made only at the highest levels of authority above installation level. Preceding sections of this study deal with such problems of authority, jurisdiction and decision-making at Department of Army and major command levels. In this section, these problems are viewed in the context of the military installation and its environment. This section also approaches problems of interim authority, temporary jurisdiction and hasty decision-making.

b. Command Relationships/Jurisdiction. Memoranda of Understanding between FBI Special Agents In-Charge and Military Installation Commanders must define, specifically, when and how FBI and military authorities will interact to insure effective operational procedures during terrorist events. To this, it is suggested that analysis, recommendation and implementation of military solutions to counter terror during events remain the responsibility of the Military Installation Commander, except in those instances when experienced FBI personnel are greater in number than those available from military sources, at which time the FBI could assume some direct control. When sufficient experienced military personnel exist it is suggested the FBI assume an advisory role.

Because no two terrorist events are alike, the relationships between the senior FBI official (Special Agent In Charge) and an Installation Commander should be a personal one, so that guidelines expressed in Memoranda of Understanding are clearly fathomed and so that one can safely act in the absence of the other, especially in the early moments of an event when time-distancc precludes the immediate presence of the FBI. In some cases, FBI officials and installation commanders may agrec to establishment of joint working groups, or forces, at every level of activity from an Emergency Operations Center on down to Forward Command Post, negotiations and tactical operatior . It would appear that situational factors such as available assets, official fixed FBI locations (offices), and existing terrorist threats would serve as determinants of formal joint forces.

Official expression of U.S. policy and overall supervision of U.S. conduct during counter terror actions OCONUS remains with a high U.S. Department of State representative, in most cases a U.S. Ambassador, while direct control of U.S. forces on U.S. military installations is the responsibility of installation commanders. Here, too, a joint command and control system can emerge, with the Department of State official (Ambassador) and the installation commander performing in accordance with Memoranda of Understanding. But the extent to which OCONUS they can together or separately direct counter terror operations is largely dependent on Status of Forces Agreements (SOFA) with Host Countries. In some countries - for example, Italy - local police have authority to react to terror on U.S. installations. There, Carabinieri would prepare and conduct counter-terror actions, while in other countries - such as the FRG - U.S. military law enforcement agencies respond on installations.

Status of Forces Agreements (SOFA) express a Host Country's position toward perpetrators conducting terror on military installations or against off base military personnel. It is from these agreements that measures are adopted to prevent military actions from extending beyond Host Country legal boundaries. Additionally, several of these agreements provide for Host Country assistance. Mutual cooperation, then, is a must between Military Installation Commanders and Host Country officials.

Further, occasions could arise when a terrorist event OCONUS may thrust Military Installation Commander, U S. Department of State Official, and Host Country official, into a triumverate, a three part command and control system, where Memoranda of Understanding and Status of Forces Agreements (SOFA) act as the stabilizing factors.

The premise here is that CONUS and OCONUS the command and control component of field counter terror operations is not a black and white, one dimensional feature but a multi-faceted aspect that has to be balanced by pre-event, agreed to procedures for inter-related decision making. The separate authorities involved participate together in arriving at appropriate options for decisions, and the mechanisms for such cooperation should be culled from Memoranda of Understanding, SOFA, and realted implementing instructions. Of course, ultimate decision making must remain with the individual mandated for such by law or policy.

There is, at present, a Memorandum of Understanding between the Department of Defense (DoD) and the FBI. This document implies coordination between Military Installation Commanders and FBI counterparts and cites the FBI's role during terrorist events, CONUS. However, during visits to U.S. Army installations, CONUS, by SAI Staff it was learned that at some installations there has been contact and coordination between the two but at others there has not; and further, detailed implementing instructions for linkage between U.S. Army and FBI personnel hardly exists.

In view of emerging terrorist threats CONUS, it is recommended that ODCSPER, Hqs, Department of the Army, formulate an action program that would revitalize and enhance coordination and coooperation between the U.S. Army and the FBI at field operating levels (installations). Further support for such action can be abstracted also from Civil Disturbance Plan, "Garden Plot." Such action, it appears, should require new meetings between Military Installation Commanders and FBI officials. From these meetings should evolve local implementing instructions dealing with the following:

- command relationships and jurisdiction
- sha ing of information
- control of military operations
- organization/construction of joint-forces
- negctiating tactics
- utilization of equipment
- liaison with media and public officials.

Further, FBI Special Agents In-Charge should receive briefings to become familiar with military installations they have to mobilize too, so as to be familiar with layout and surroundings.

Similar actions should also be accomplished OCUNUS between Military Installation Commanders and the U.S. Department of State and, where applicable, with Host-Country Officials, certainly pursuant to joint review of applicable segments of Status of Forces Agreements (SOFA).

With direction and supervision of the above cited actions begun at Department of Army level, and enforced by Major Commands, near future compliance would be readily obtainable, especially since authority exists now in the standing DoD/FBI Memorandum of Understanding, and in SOFA.

c. Time factors, the Hostage-Taking Terrorist Event (Scenario) and Situational Control.

(1) Time Factors. There is a distinct relationship between the phases of a terrorist event and the degree and intensity of situational command and control that can be brought to bear in a counter terror effort on military installations. Unavoidably, it is difficult to determine who can be the first responsible leader on scene. Even if mechanisms exist to mobilize a Reaction Force, a Forward Command Post and an installation Emergency Operations Center, the first responsible counter terror agents to confront terrorists may be nearby security guards or a pair of military policemen arriving by sedan while on roving patrol. This reality cannot be dismissed, and instead should be viewed as an initial 'official' reaction phase during which opportunity exists to estimate the terrorist situation and begin a transition into subsequent phases when a viable Reaction Force could arrive on scene. As stated elsewhere in this study, it is important and practical that all military police personnel have training in methods for dealing with terrorists. In civilian police situations, the first police officer to arrive on scene during a criminal or terrorist hostage-taking/barricade situation is designated the 'initial commander' of police forces until a special detail trained for such situations arrives. Other ranking officers arriving on scene have authority to assume situational control but normally only provide guidance or advice, allowing the 'initial commander' to stay in charge until relieved by the special detail. It is suggested this system be U.S. Army practice in order to sustain as much continuity as possible during the early flow of activities.

(2) The Hostage-Taking Terrorist Event (Scenario). A later par graph in this section discusses elements that can be mobilized on installations to counter terrorism. These elements are listed below in reference to sequences of some major type hostage-taking terrorist events that could occur on installations, purpose: to relate time-, or chronological-, sequences of terrorist events to the element, or

elements, that should be exercising direct situational control within the framework of the sequence, and to outline major duties and responsibilities in the flow of actions, or sub-events. By direct, in this case, is meant that element that should be in direct contact, or confrontation, with the terrorists. The type terrorist event treated is worst case, that is, a hostage-taking/ barricade situation by politically motivated terrorists with specific demands. From the point of view of counter terror forces, events are:

- Initial Response Phase
- Negotiation Phase
- Assault Phase

The Initial Response Phase is that period during which U.S. military personnel become aware of a terrorist committed act and prepare to counter the act through peaceful persuasion or military force. The Negotiation Phase, occurring during hostage-taking situations, is that stage during which military or other official personnel interact with terrorists to reduce factors of potential violence and increase the probability of safety for hostages while bargaining (negotiating) for their release. The Assault Phase occurs when it has appeared that only a military solution can bring about the release of hostages with less harm coming to them than through the application of other solutions, or when anything less than a military solution has been analyzed to have greater negative impact on human lives elsewhere.

Below, in sequence and scenario fashion, is a breakout of the above mentioned phases.

Initial Response Phase

- Terrorists sieze building and take hostages.
- Nearest available military policemen arrive on scene.
- Military policemen estimate situation
- Military policemen report incident to higher headquarters (MP Operations Desk).

- MP Operations Desk alerts Installation Headquarters Operations Center, the Provost Marshal; next, subordinate Commanders of elements of a predesignated Reaction Force.

- Duty officer at Installation Headquarters Operations Center alerts installation Commander, then, if in CONUS, contacts the FBI, next the Army Operations Center (AOC), Headquarters, Department of the Army, and the next higher command.

- OCONUS, the Installation Headquarters Operations Center contacts the Major Command, e.g., Headquarters, Usareur.

  (Note: alert notifications cited are in accordance with Army Regulation Number 190-40)

- Installation Headquarters Operations Center converts to Installation Emergency Operations Center (IEOC).

- Initial on scene commander (ranking military policeman) sustains contact with terrorists and in accordance with learned, pre-established procedures attempts to ascertain information toward a precise estimate of the situation.

- Provost Marshal, or designated representative, arrives on scene at nearby location to establish Forward Command Post, assuming forward operational control as Commander. Initial, now former, Commander remains at Command Post to provide information and assistance.

- Security and reconnaissance personnel of the pre-designated Reaction Force arrive on scene and establish physical security cordon and reconnoiter area to determine best access and egress to and from the terrorist target (building with terrorists and hostages).

- Tactical elements of predesignated Reaction Force moves to assembly area beyond sight or recognition of terrorists and prepares for possible assault operations.

- Forward Command Post establishes communications with Installation Emergency Operations Center (IEOC).

- Installation Commander arrives at IEOC to command counter terror operations, first obtaining an estimate of the situation from the Provost Marshal.

- Forward Command Post, in accordance with learned predesignated procedures:

- sustains contact with terrorists and determines, if possible:
  - number of hostages and who they are, and their condition.
  - precise interpretation of terrorist demands.
  - number of terrorists, type terrorist group, and positions of terrorists in the building, and movement patterns of both terrorists and hostages.
  - names of terrorists, especially the leaders.
  - terrorist behavior characteristics (e.g., nervous, tense, easily excitable, or unemotional).
  - terrorist weapons, explosives, equipment.
- analyzes reported best access and egress to and from building (reported by elements of the Reaction Force).
- develops tactical military options for use by tactical elements.
- determines if available resources will support planned tactical military options.
- begins formal negotiations with terrorists (note: terrorists may reject the assigned Negotiator and request to negotiate only with Installation Commander or other official party).
- reports results of all of above to IEOC.

- Senior FBI official arrives at IEOC and receives briefing on situation from Installation officials. The FBI agent will work closely with counterterror forces providing guidance and assistance.

Negotiation Phase

- Negotiating Team, or Negotiator, sustains contact with terrorists and buys as much time as possible from terrorists for the consideration of demands.
- IEOC forwards clarification of demands to AOC/DA and awaits guidance as to how the U.S. government will react. OCONUS, reports to OPNS Center, Major Command.

- Forward Command Post forwards to IEOC recommended tactical military options with estimated risk factors.

- IEOC analyzes tactical military options and determines best option, then alerts Forward Command Post of the option selected.

- Forward Command Post alerts Leader, Tactical Element and provides him with the military option plan although permission to conduct such plan is yet to be granted.

- Leader, Tactical Element, returns to rear assembly area and briefs element to conduct the plan. Element obtains additional equipment, if needed, and undergoes full preparation, rehearsing actions repeatedly.

- FBI official and/or Installation Commander (i.e., on command perogative) may move to Forward Command Post. However, it should be noted the appearance of additional authority may be viewed by terrorists as an indication of impending violent action.

- AOC/DA forwards to IEOC a decision on use or non-use of tactical military option. IEOC reports decision to Forward Command Post (FCP). Cmdr, FCP alerts Cdr, Tactical Element.

  (if a decision is made to conduct tactical military operation, the following:)

  - Assault Phase:

    - Tactical Element completes rehearsals, re-groups at Assembly Area, establishes mobile command post and informs Forward Command Post when ready to embark on military operation.

    - On order, Tactical Element moves as covertly as possible from Assembly Area to its objective (building with terrorists and hostages).

    - Forward Command Post alerts support elements, e.g., medical, transportation, etc., to embark on supportive missions.

    - Tactical Element conducts assault to free hostages and take prisoners.

    (if a decision is made NOT to conduct an assault, NEGOTIATION continues)

(3) Situational Control. As stated, event and post event terror/counter terror activities include, sequentially, three basic categories: Initial Response Phase, Negotiation Phase, and Assault Phase. In each of these phases there are progressive links of command and control elements which exercise direct or indirect, that is, operational or decision making situational control. These elements cover four distinct areas in the range of command and control procedures, and these are:

- Direct Tactical Control
- Indirect Tactical Control
- Overall Strategic Decision Making Control
- Overall Policy Effects Control

Figure One, page C-16 depicts these elements and their relationships as procedural mechanisms to command and control elements.

The outcome of terrorist events rests on the effects of counter terror situational control; therefore, players in command and control linkages described must be fully aware of limitations imposed upon them by policy direction. Their duties and responsibilities should be spelled out clearly in Installation and Special Unit SOP, and all personnel involved should have formal schooling and training directly proportionate to the tasks that policy will require of them.

d. Formalizing a Chain of Command. The ladder of direction for countering terrorism on military installations should be a basic structure of authorized officials and directives. Analysis of cases involving terrorist objectives and counter terror actions show that the following vertical structure is more adaptable across the spectrum of type terrorist acts as a viable chain of command:

Figure 1

"Evolution of S tuational Control/Counter Terror"

(Hostage-taking Incident)

"Phase"	Exercising Direct Tactical Control	Exercising Indirect Tactical Control	Exercising Overall Strategic Decision-Making Control	Exercising Overall Policy Effects Control
Initial Response Phase	First Authority On-Scene (MP) Cdr, Fwd CP (Provost Marshal)	Installation Opns. or Duty Officer until the arrival of Cdr, IEOC (Instal Cmdr, or early-on designated senior representative)	Cdr, IEOC (as left of this column)	
Negotiation Phase	Cdr, Fwd CP (Provost Marshal) Negotiator	Cdr, IEOC* (Instal. Cdr)	Cdr, IEOC*	Hqs, DA (AOC); or, as OCONUS sitautions, Major Command or US Dept of State (Embassy)
Assault Phase	Cdr, Fwd CP Cdr, Tactical Element	Cdr, IEOC*	Cdr, IEOC*	As Above

* FBI official advises and assists

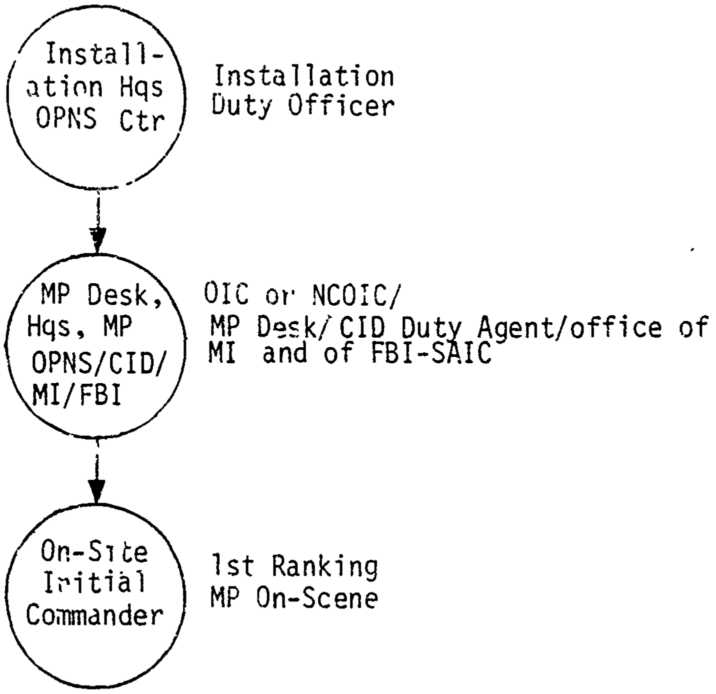
Command and Control	Parallel Mechanism(s)
Commander, US Army Installation... FBI advises and assists.	National policy . . . DOD/FBI Memorandum of Understanding . . . Installation/FBI Memorandum of Understanding . . . Installation SOP/reaction force SOP . . . Relative US Army regulations and directives
Commander, Reaction Force	Installation SOP/Reaction Force SOP
Subordinate Commanders, Reaction Force	Installation SOP/Reaction Force SOP
Negotiator	Reaction Force SOP

Excluded from this structure are the command and control element(s) that would exercise situational control during the Initial Response Phase. When added, a vertical structure - side-by-side graphically with inherent command locations - appears as below:

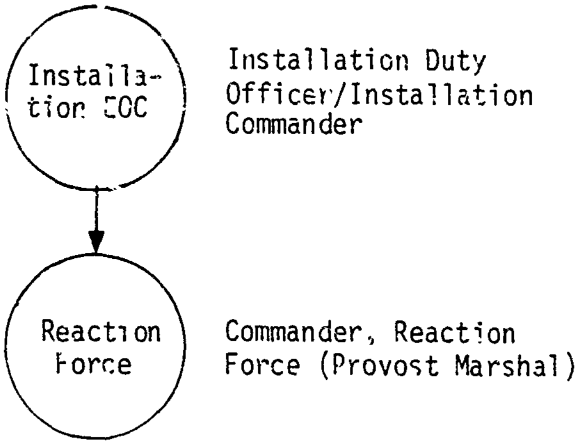
(Note: this MODEL is NOT presented as a panacea for dealing with terrorism organizationally on installations; rather, as cited, it is the MODEL which in SAI's case-by-case simulations appeared to have greater flexibility and success in controlling operations)

Initial Response Phase

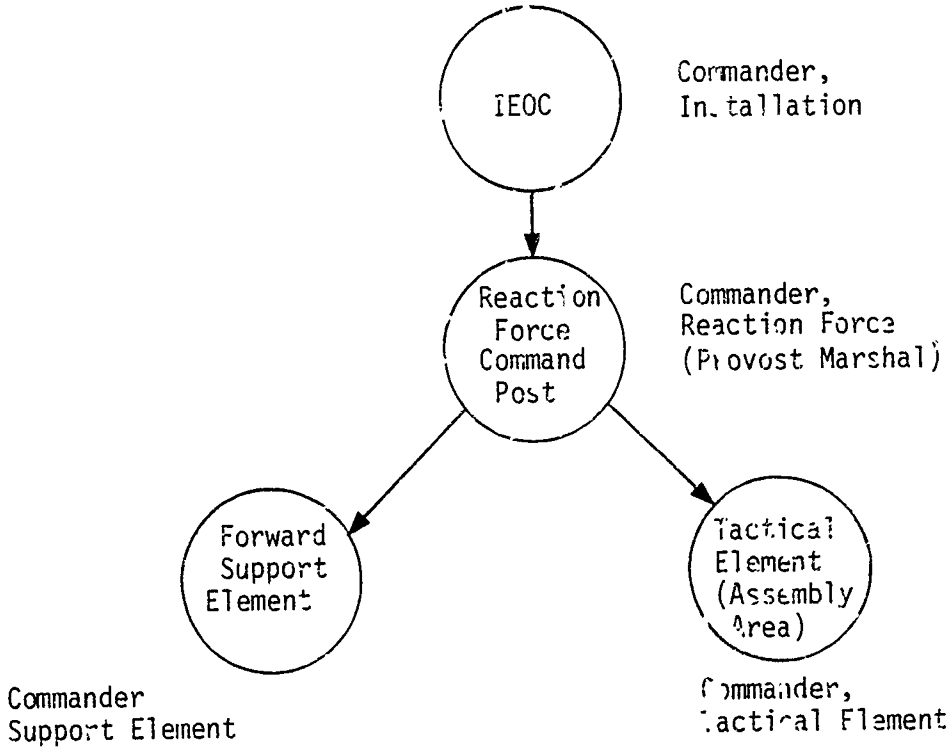
- sub-phase one (recognition of terrorist act)


Install-ation Hqs OPNS Ctr
Installation Duty Officer
MP Desk, Hqs, MP OPNS/CID/ MI/FBI
OIC or NCOIC/ MP Desk/CID Duty Agent/office of MI and of FBI-SAIC
On-Site Initial Commander
1st Ranking MP On-Scene

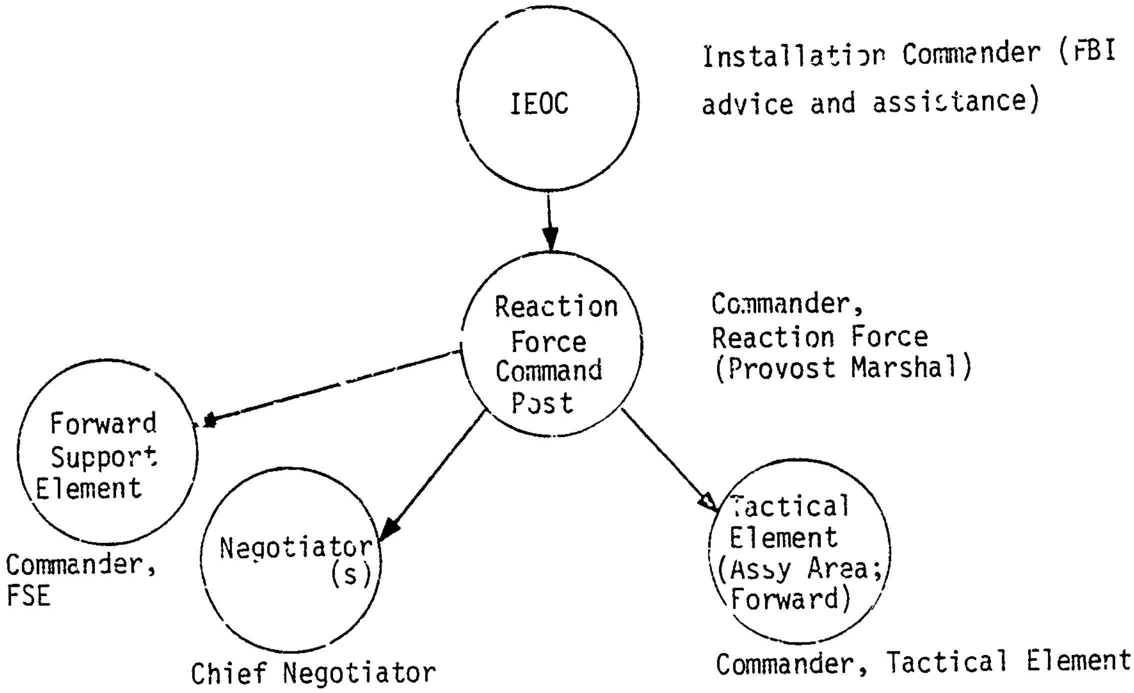
- sub-phase two (Establishment of IEOC and Forward Command Post/Arrival of Installation Commander at IEOC)


Installa-tion EOC
Installation Duty Officer/Installation Commander
Reaction Force
Commander, Reaction Force (Provost Marshal)

- sub-phase three (Elements of Reaction Force arrive at designated locations)



Negotiation Phase/Assault Phase



The negotiator is considered a key element in the chain of command because in a Negotiation Phase he is in direct contact with, and can influence, the counterterror target (i.e., the terrorists).

In formalizing this chain of command, several questions arose which deserve comment. First, and perhaps most striking, has been dealt with in preceding pages but requires further analysis. "What should the FBI's role in counterterror operations on a military installation include?" On the one hand, the question is nearly "moot" since law provides the FBI with jurisdictional authority. But, the FBI suffers some disadvantages in being able to carry out obligations on military installations during terrorist events, especially early on. Time, distance and lack of intimate knowledge of military capabilities are certainly deterrents to total FBI effectiveness. In several instances, FBI officials are located several hundreds of miles from military installations and cannot be on scene during crucial moments when initial response to terrorism must be thorough, balanced and proficient; thus, the need for the aforementioned Memoranda of Understanding.

Other questions dealt with in formalizing a recommended chain of command were:

- Should Provost Marshals always command Reaction Forces? Could a non-law enforcement field grade officer assume this responsibility?

- Snould a Deputy or Assistant Reaction Force Commander have full charge of the Tactical Element of a Reaction Force or should the Tactical Element have a leader who has no other function than to lead the Tactical Element?

- What should minimum grade structures be?

To arrive at answers to these questions, the following advantages and disadvantages were reviewed:

Cdr, Installation	Senior influential military officer . . . expertise and thorough familiarity w/military operations and available assets and resources	other major installation duties may have to be set aside
Dep or Asst Cdr, Installation	Can specialize moreso than Cdr during pre-event periods . . . attention less divided . . . expertise and thorough iarity w/military operations and assets and resources . . . can free Cdr to serve on scene, if necessary, as Negotiator.	Less significant advantage in dealing w/external and/or higher authorities

Chain of Command	Advantages	Disadvantages
Provost Marshal (Cdr, Reaction Force)	Law enforcement and counter terror training expertise . . . knowledge of assets, resources . . . legal expertise . . . intimate knowledge of area of operations	Diverted from other major duties
Non law enforcement Cdr, Reaction Force	Frees PM or other key law enforcement officer for other major requirements	less, if any expertise in counter terror, legalities, law enforcement . . . less knowledge of assets, resources
Dep or Asst Reaction Force Cmdr also as Tactical Element Leader (w/Asst Tactical Element Leader Conducting Assault OPNs)	Provides Reaction Force Cdr direct intimate link w/Tactical Element . . . enables balanced control of Tactical Element's Security and Assault units	diverted from other forms of leadership assistance at fixed cmd post

Preceding paragraphs reflect that in light of the above and other variables, the chain of command selected would provide greater control and flexibility. The below restatement of this chain of command includes basic rationale for selection:

Permanent Title	Counter-terror Mode	Location	Rationale
Installation Cdr	Chief, Military Operations	IEOC	Current Cdr of all MIL assets and resources . . highest official link to other authorities
Dep. Inst. Cdr	Dep. Chief, MIL. Operations	IEOC	(second to above)
Provost Marshal	Cdr, Reaction Force	Fwd CP	Law enforcement, legal & counter terror expertise; intimate knowledge of assets & resources

Permanent Title	Counter-Terror Mode	Location	Rationale
Dep. or Asst PM	Cdr. Fwd Spt Element	Fwd CP	As above
Cmdr, MP Company	Cdr, Tactical Element	Rear Assy Area/Tactical - Mobile CP	Linkage between Fwd CP and Tactical Element
Platoon Ldr, MP Company	Ldr, Assault Unit (Tactical Element)	Rear Assy Area/Area of Target	OIC w/single focus
Platoon Ldr, MP Company	Ldr, Security Unit (Tactical Element)	Vicinity target area/	OIC w/single focus

(FBI official, not in chain of command, is "operational consultant")

On major installations, fitting the above into a counter terror force would meet with little difficulty; however, at smaller installations and sites company grade officers may have to fill positions suited for field grade, and senior NCO's may have to serve in company grade positions. Because of the sensitivity of terror/counter terror and ensuing national and international implications, officers of the higher grades should be filling key positions. On more-populated installations, recommended grade structuring follows:

Title	Recommended
Commander, Installation (Chief, Military Operations)	Colonel (0-6) to Major-General, unless lower grade authorized.
Provost Marshal (Cdr, Reaction Force)	Field-grade officer unless company-grade (Captain) is highest grade available for position.
Dep or Asst PM, Office of Provost Marshal (Cdr, Forward Support Element)	Captain

Title	Recommended
Company Cmdr, MP Company (Cdr, Tactical Element)	Captain
Platoon Ldr, MP Company (Ldr, Assault Unit of Tactical Element)	1-LT
Platoon Ldr, MP Company (Ldr, Security Unit of Tactical Element)	1-LT

III. ORGANIZATION

Type Forces. A military installation counter terror infrastructure should emerge from existing assets with speed, alacrity and minimum re-organization. The previous sub-section, or paragraph, stated that against near term and future terrorist threats, CONUS and OCONUS, existing military organizations have personnel and resources available to conduct counter terror missions pursuant to effective training programs. It is unlikely that soon, or by 1983, terror will require organizations dedicated solely and continuously to the counter terror mission. This conclusion is based on analyses of several organizational concepts with matching terrorist event probabilities. These concepts are:

- Newly-activated, dedicated TOE/TDA counter terror force, to include an internal command structure, and tactical, security and support elements.

- Newly activated, dedicated TOE/TDA counter terror tactical and security elements, commanded, controlled and supported by external existing authorities.

- Conversion, or fusion, of elements of current TOE/TDA units into dedicated counter terror forces for indefinite period.

- Designation of existing personnel and/or units to serve in a counter terror mode when need arises/on-call.

Balancing the terrorist threat against cost factors such as manpower, physical resources, time, planning and training, to entertain the first three concepts cited would be to engage developmental models far too costly in relation to real world need. The latter concept, more cost effective, relies on existing personnel and resources backgrounded for the counter terror mission within a framework of response realism. Indeed, the former concepts would provide better trained and specifics oriented counter terror elements, but only in a framcwork of illusions about terrorism along with a lack of realism about prioritizing funds and resources.

Recommended, then, is not a new organization in the force structure but the development of on-call missions for organizations already TOE/TDA-authorized.

Since terrorism on military installations is likely to be of lower-level violence (small teams with individual weapons) existing U.S. Army law enforcement units appear to be most suited to enact counter terror tactics under the supervision of Provost Marshals and Installation Commanders. In brief, current TOE/TDA's for Military Police Companies include personnel and equipment for expected stand-off counter terror activities. Personnel of these units selected to perform per the latter concept could continue in their normal TOE-prescribed duties, mobilizing to counter terror in accordance with contingency plans and for periodic training.

This recommendation does not preclude a need for the U.S. Army to develop plans for counter terror force structures outside the law enforcement realm. After all, the imperative, or cue, for structuring counter terror elements comes from the type of terrorist act committed. The 1976 Israeli raid at Entebbe required meticulous task forcing of regular combat elements. It is possible that terrorist acts against U.S. Army personnel or others on military installations could require platoon or company-size forces such as Ranger units, or that aspects of a unique incident could necessitate conversion of a Special Forces

Operational Detachment "A" to a counter terror mode. Such considerations cannot be ignored, even though existing threat assessments spread much doubt over the probability of terrorist acts against the U.S. Army frequently necessitating combat task forces. Into 1983 and beyond, it appears that most terrorist acts against the U.S. Army can be confronted successfully with in-being law enforcement assets.

In designing a response configuration for military installations, two basic components were realized to serve the following two objectives:

- Crisis-Management
- Tactical Response

The two components of the configuration are:

- Installation Emergency Operations Center (IEOC); and
- Special Reaction Force (SRF).

These components include foundations for independent action against, or inter-action directly or indirectly with, terrorists. Below is a description of missions and capabilities of these components under an umbrella titled, Counter Terror Force Structure. A MODEL, this organization should be viewed as one of several workable configurations. SAI, however, has noted that in simulations it best suited personnel resources, assets and capabilities available at most installations.

Counter Terror Force Structure

- Components
  - Installation Emergency Operations Center (IEOC)
  - Special Reactic Force (SRF)
    - Forward Command Post
    - Forward Support Element
    - Special Reaction Team (SRT-Tactical Element)
      - Assault Unit
      - Security Unit

- Requirements

  - IEOC

    - MISSION: Command and control military response to terrorist acts on military installations.

    - RESPONSIBILITIES:

      - Pre-event: Develop counterterror contingency plans/SOP's

      - Ascertain precise estimates of the terror/counter terror situation throughout the response period.

      - Conduct assessments of military "response options" and recommend the most favorable to Department of Army for concurrence or non-concurrence.

      - Conduct operational planning and provide operational and support guidance to Cmdr, SRF.

      - Establish communication links to Major Command and/or to AOC, DA.

      - Coordinate support activities.

      - Effect liaison with Public and Media officials.

      - Organize post operational plan to support needs of released hostages and to organize captured terrorists.

  - Special Reaction Force (SRF)

    - MISSION: Conduct on-site operations against terrorists on the military installation.

    - RESPONSIBILITIES:

      - Establish on site Forward Command Post.

- Establish and direct Forward Support Element to:
  - secure area of operations
  - negotiate with terrorists
  - develop safety measures for hostages throughout the response period
  - gather intelligence
  - coordinate logistics and medical support
  - establish communication links with the IEOC and the SRF's Forward Support components, and the SRF's Tactical element (SRT)
  - provide continuous estimate of the situation to the IEOC
  - recommend "response options" (tactical) to the IEOC
  - conduct, only ON ORDER, tactical operations.

Composition. The IEOC, in essence, should be an installation's in-being Operations Center augmented to deal with terrorist situations. When manned fully, principals should be pre-designated on call representatives of the installation's major command and staff elements that match disciplines required to counter terrorism. It should also, as closely as possible, match counterparts in the AOC/DA or major command. To sustain operations, this structure should, at a minimum, include the following:

- Installation Commander.

- Dep or Asst, Installation Cdr.

- Chief of Staff, Installation. Coordinates IEOC internal operations.

- Senior FBI official/SAIC...advisor

- IEOC Augmentation. OIC of:

● Intelligence. Provides production and analysis of intelligence collected not only from operational site but from other sources. On major installations, where assets exist, directs "all-source" intelligence center;

● Operations. Provides estimates of tactical options and develops and refines operational plans;

● Personnel. Provides guidance on availability, utilization and care of personnel;

● Logistics. Provides coordination of equipment and transportation support actions;

● Public Affairs. Effects liaison with Media and private sector officials. Note: This officer and assistants may be positioned at the Forward Command Post (situation-dependent);

● Legal Affairs. Provides advice and recommendations on legal implications;

● Communications-Electronics. Insures effective communication systems, links, appropriate equipment. rigs.

● Facility Engineer. Provides information. re. buildings and sites.

- Behavioral Psychologist. (Can be military, or locally contracted, or on call from other installation). Provides guidance for on site Negotiator.

The counterterror augmented IEOC configuration that serves responsibilities and requirements of the IEOC mission includes three basic elements. These are:

- Command Element Team
- Crisis Management
- Operational Staff

The aforementioned principals should comprise these elements as follows:

- Command Element (decision Making)
  - Cdr, Installation
  - Dep. (or Ass't) Installation Cdr.
  - Chief of Staff, Installation
  - FBI official/SAIC
- Crisis Management Team (Analysis, Decision Making)
  - Dep. (or Ass't) Installation Cdr. (directs team)
  - Intelligence Officer
  - USACIDC officer - special agent
  - Operations Officer
  - Logistics Officer
  - Legal Officer
  - Psychologist
  - Facility Engineer

- <u>Operational Staff</u>. Principals, and staff representatives . . .
  - COS, Installation (. . . directs:)
    - Intelligence (OIC and Staff)
    - Operations (OIC and Staff)
    - Personnel (OIC and Staff)
    - Logistics (OIC and Staff)
    - Public Affairs (OIC and Staff)
    - Legal Affairs (OIC and Staff)
    - Communication-Electronics (OIC and Staff)

The purpose of the <u>Command Element</u> is obvious: to direct action, and to recommend to higher authority the most favorable option or options for a counter terror strategy.

The <u>Crisis Management</u> team provides the <u>Command Element</u> with a breakout analysis of recommended options, so that the Chief, Military Coordination (Cdr., Installation) can deliver to higher authority the best option, or options, and so that subsequent decisions and actions can be analyzed thoroughly and be fully coordinated. This team should be directed by the Deputy, or Ass't., Installation Commander, and commence as soon as a clear estimate of the situation is received at the IEOC from the Forward Command Post of the Special Reaction Force, and certainly upon each significant sub-crisis.

The Operational Staff, third element of the IEOC, includes continuous hands-on working staff members who are responsible for the IEOC's internal operational and support duties. The Chief of Staff (COS) of the Installation should be responsible for direction of these personnel.

No doubt, not every major installation CONUS and OCONUS will have an organization available to immediately convert to the counter terror force structure described herein. Some installations may not have a Chief of Staff but instead an executive officer and in many instances an installation's senior 'Operations' officer may also be the 'Intelligence' officer. Thus, the above is recommended as a MODEL from which appropriate departures (modifications) should occur.

IEOC Facilities, Equipment and Special Items for the IEOC need be no different than those required for an installation's operations center during emergency category I events, although some additional communications frequencies may be needed and certain items peculiar to the terrorist situation would reed be available, such as:

- Building and floor plans (blueprints) of the barricaded building and adjacent buildings (to include basements and any other underground areas).

- Maps and/or diagrams of the installation's airfield and designated helipads (to include blueprints of buildings and hangars) in the event terrorists and hostages, via demand, gain passage to move toward aircraft.

- Maps and/or diagrams of nearby commercial airfields, heliports, re. above situation.

- Maps and/or diagrams of buildings and other facilities along obvious exit routes from barricaded building and along routes to airfield and/or helipad.

- If available, files on terrorist organizations and practices.

This IEOC configuration, pitted against several terrorist situations, insures in-depth coverage against the unexpected as well as the obvious. Situation-dependent, its size may grow. For example, as discussed earlier, FBI officials may wish to fuse FBI staff into functional sections, and USAF or civilian commercial airfield personnel may be required if there are needs for long-range aircraft. Thus, it is imperative that Installation Commanders develop contingency plans that include appropriate configurations for the IEOC, using the MODEL herein as a base start. SOP must be laid down carefully to insure quick and efficient fusions of additional personnel.

Special Reaction Force (SRF)

The Special Reaction Force (SRF) is the counter terror blow impacting at the crisis-point. It should be a force of modular components that can be mobilized quickly to reach event locations and prearranged sites. These structural units must gain control of terrorists in any military or behavioral context. At the minimum - that is, for installations rated less vulnerable to terrorism than others - a Special Reaction Force should include the following:

- Forward Command Post (FCP)
- Forward Support Element (FSE)
- Special Reaction Team (SRT)

The Forward Support Element commences its operations from the location of the Forward Command Post as directed by the Commander of the Special Reaction Force (Provost Marshal) and includes the following:

- Security and Reconnaissance Team
- Supply Section
- Signal Section
- Medical Section
- EOD Detachment

The Security and Reconnaissance Team must early on cordon the operational area and make certain that bystanders and onlookers are out of range of any fire or danger. Elements of the Team must also develop intelligence information as quickly as possible, reporting to the Command Post entries to the target building, escape routes, characteristics of the building, and facts about the terrorists and hostages.

The Negotiating Team should include two or more trained Negotiators who can be positioned on site to converse directly with terrorists to ascertain clarity of terrorist demands, and subsequent proposals and counter proposals; to state U.S. Army and U.S. Government positions, describe actions to be taken, and to supervise or assist in supervising the delivery of hostages and products; to gain information about terrorists and hostages; to stall; and to regulate or modify terrorist behavior. More than anyone else in the counter terror force structure, negotiators, prior to an assault phase, are the cutting edge, the prime forward control factor. Negotiators must attempt through direct or subtle means to upstage terrorists and steal their initiative, to wrest control from them and lead the situation to a conclusion favoring the U.S. Government. However, negotiators should not be decision makers. It is the inability of negotiators to make decisions that widens their field of communications and extends their opportunities to develop rapport with terrorists. Still, terrorists may reject assigned negotiators and demand to bargain only with an authority who can make decisions. When this occurs, assigned negotiators should serve as assistants to the preferred negotiator.

The role of the Supply Section should be to acquire and deliver equipment and rations to operating locations, as directed by the Forward Command Post. It is likely that rations and equipment will have to be provided to the terrorists and to hostages.

Communications support, that is, the establishment of lines, and creation of a command and control net linking the Forward Command Post to the Forward Support Element's various components and to the Special Reaction Team, is the responsibility of the Signal Section.

The Medical Section, located initially at the Forward Command Post, must be mobile and have the capability to treat terrorists as well as hostages and SRF personnel. A "dust-off" capacity should be established for the seriously wounded if appropriate facilities are not nearby.

The EOD Detachment assumes a role in counter terror when bombs or other explosives are required to be identified and defused.

En toto, a Forward Support Element need not comprise more than 35 personnel. A suggested breakout is:

● Cmdr. Fwd Spt Element:	1
● Security and Reconnaissance Team	
- Team Leader:	1
- Security Unit:	11
- Reconnaissance Unit:	3
	15
● Negotiating Team	
- Chief Negotiator:	1
- Negotiator:	1
- Asst. to Negotiator and Driver:	1
	3

- Supply Section

- Supply NCO:	1
- Asst. Supply NCO:	1
- Supply Clerk:	2
- Drivers:	2
	6

- Signal Section

- Communications Officer, WO, or Senior NCO:	1
- Communications Specialist:	2

- Medical Section

- Surgeon:	1
- Medical Officer:	1
- Medics:	3
- Drivers:	2
	7

- EOD Augmentation Team (not included in above personnel accounting).

The Special Reaction Team (SRT) is the tactical element of the SRF, similar to the Special Reaction Team that military law enforcement agencies formulated long before the civilian counterpart, SWAT. When mobilized it should move to an Assembly Area sufficiently distant from the target area (terrorists) so as to avoid detection of its existence. It's purpose is to sieze, ON ORDER, a target barricaded, or defended otherwise, by terrorists so as to capture them and to free hostages, and to engage terrorists by fire, ON ORDER, as opportunities arise.

Below are elements of a Special Reaction Team (SRT) for the counter-terror mode:

- SRT Command Unit
- Assault Unit
- Security Unit

The SRT Command Element need include only the SRT Commander and a driver/radio-operator. The Assault Unit must be capable of fast and furious entry and offensive tactics, and accurate weapons firing. The Security Unit must be able to provide support by fire during an assault, and/or independent sniper fire. Appropriate make up for the latter two is shown below:

● SRT Cmdr:	1
● Driver-Radio Operator:	1
● Assault Unit	
- Leader:	1
- Automatic Rifleman:	2
- Rifleman:	4
- Grenadier:	2
- Radio Operator:	1
- Driver/Radio Operator:	1
TOTAL	11
● Security Unit	
- Leader:	1
- Automatic Rifleman:	3

-	Snipers:	5
-	Driver/ Radio Operator:	1
	TOTAL	11

SRT personnel require diversified training, including wall-climbing and rapelling, special weapons, night devices, use of demolitions, explosives and riot control agents, water cannons, battering rams, rescue procedures, and first-aid.

Forward Command Post. The Forward Command Post effects command and control of on site military operations against terrorists as directed by the IEOC. It serves as a hub, or focal point, for delivery of orders and commodities to the SRF's subordinate elements, and collects, analyzes and disseminates intelligence information.

No more than 8 personnel need constitute the Forward Command Post, and less can man it on sites or lesser installations where fewer personnel exist. On most installations, a Forward Command Post might include the following:

- Commander, Special Reaction Force (Provost Marshal) - 1
- Deputy Commander, Special Reaction Force and Commander, Forward Support Element (Deputy, or Assistant, Provost Marshal) - 1
- SRF Operations Officer (Operations Officer, Office of Provost Marshal) - 1
- Intelligence NCO (E-8 or E-7) - 1
- Intelligence Specialist (NCO, E-5 or above) - 1
- Communications Specialist - 1

- Driver - 1
- Clerk - 1

As to proper location, the Forward Command Post should be in a closed or protected area from where the target area (location of terrorists and hostages) can be observed.

Excluding IEOC personnel, the Counter Terror Force Structure for a major installation as described above comprises 63 personnel. A summary breakout of this structure is below:

"Counter Terror Force Structure"

- Installation Emergency Operations Center (IEOC)
  - Command Element
  - Crisis Management Team and Operational Staff
- Special Reaction Force (SRF)
  - Forward Command Post
    - SRF Commander
    - Dep. SRF Commander and Cmdr, Forward Support Element
    - Operations Officer
    - Intelligence NCO
    - Intelligence Specialist
    - Communications Specialist
    - Driver
    - Clerk
  - Forward Support Element
    - Security and Reconnaissance Team
      - Team Leader

    - Asst. Team Leader
    - Security Unit - 10
    - Reconnaissance Unit - 3
  - Negotiating Team
    - Chief Negotiator
    - Negotiator
    - Asst. to Negotiator and Driver
  - Supply Section
    - Supply NCO
    - Asst. Supply NCO
    - Supply Clerk - 2
    - Driver - 2
  - Signal Section
    - Communications Off., WO, or NCO
    - Communications Specialist - 2
  - Medical Section
    - Surgeon
    - Medical Officer
    - Medics - 3
    - Driver - 2
  - EOD Augmentation Team
- Special Reaction Team
    - SRT Command Post
      - SRT Commander
      - Driver and Radio Operator

- Assault Unit
  - Leader
  - Automatic Rifleman - 2
  - Rifleman - 4
  - Grenadier - 2
  - Radio Operator
  - Driver
- Security Unit
  - Leader
  - Automatic Rifleman - 3
  - Snipers - 5
  - Radio Operator - 1

As stated earlier, small sites and lesser installations may not have assets to develop the force structure shown above. Commanders of such sites or installations should, however, be directed by policy to formulate and arrange contingency measures to draw force assets from the nearest available military or civilian law enforcement sites, installations or agencies. For example, nearby active military posts and state or local police could serve this purpose well.

Tactical Reserves may become necessary during an assault phase. Where personnel are available, a second Assault Unit, identical in make up and capability to that of the assigned SRT, should be mobilized along with the SRT and underge assault preparations with its front line counterpart.

Special Reaction Force Equipment. Equipment for the elements of the Special Reaction Force need include only standard, low technology items that can be found on most installations or sites with the possible exception of an armored vehicle.

IV. SPECIAL OPERATIONAL TASKS

Analyses of counter terror operations conducted throughout the world by military forces and police agencies since 1970 uncover functional task-areas which require examination subsequent to development of theory (policy) and practice (operational response). The task areas ascertained from SAI study of terrorist cases are:

- Command and Control; command relationships; the decision making process; task forcing/organizing.
- Intelligence (collection, dissemination, analysis)
- Negotiating
- Communications
- Liaison with Media and Public Officials
- Support

Measures increasingly evident from study of cases grew not so much from what was achieved by counter terror forces, but from what was NOT achieved. No doubt, a great deal remains to be known about dealing with political, ethnic, racial or pathological terrorists, however, the sampling of incidents studied, as well as simulated hypothetical 1977/1983 terrorist events, provided a hefty number of lessons and lessons learned. Among the real incidents studied were:

- PFLP hijacking of aircraft, LOD airport, 1972, less than two months prior to infamous JRA/PFLP LOD airport massacre.
- Black September attack during Munich olympiad, 1972.
- Tupamaro kidnapping of U.S. Advisor Daniel A. Mitrione, 1970.
- Black September seizure of U.S. Envoy to Sudan, Cleo A. Noel, subsequent murder, 1973.
- PFLP attack, Tel Aviv hotel, 1975.
- Metropolitan area police cases, District of Columbia, New York City, San Francisco, 1975-1976.
- South Mollucan seizure of Indonesian Consulate, Amsterdam, 1975.
- Hostage - taking, OPEC Ministers Meeting, Vienna, 1975.
- Coordinated terrorist actions, Washington, D. C., 1977.

The first item of operations task interest listed above - command and control, etc. - has been covered in preceding pages of this section. Thus, the second item - intelligence - begins this portion of analysis.

Intelligence. During a terrorist event, intelligence information is of prime importance in perfecting countermeasures. In hostage-taking situations, both assault and negotiation tactics benefit from early information about terrorists. It is because of this that SAI has incorporated into its counter terror organizational MODEL, a small reconnaissance team, or function, to aid the intelligence gathering effort and why, too, a list of "essential elements of information" (EEI) should exist to aid such effort. More precisely, intelligence collection during events should serve the following needs·

- information for imminent tactical use by counter terror forces.

- information to flesh out a psychological profile of the terrorist leader, and of the group as well.

- information about general and specific terrorist modus operandi (for both present and future use).

- general and specific information about hostages.

The gathering of intelligence information during events should begin immediately on recognition that an event has taken place and should continue well beyond the event with interrogations of any captured terrorists and debriefings of hostages and counter terror force participants who confronted terrorists directly. Negotiators should also be debriefed. A list of intelligence collection sources is as follows:

- Initial Commander (1st ranking MP on scene).

- Bystander/witnesses of early terrorist actions who have not been taken hostage.

- Security and Reconnaissance Team of the Forward Support Element (SRF).

- Early-released hostages.

- Negotiators.

- Special Reaction Team.

- Facility personnel (those with intimate working knowledge of barricaded area or areas to which terrorists may relocate, e.g., airfield).

- Remaining hostages.
- Local or other personnel who may be familiar with terrorists or terrorist organization... Note: FBI and USACIDC should attempt to locate such personnel

The on scene intelligence gathering coordinator in the SAI organizational MODEL is a trained non-commissioned officer assigned to operate within the Forward Command Post of the Special Reaction Force. Upon arrival at the scene, this individual should begin to obtain information in accordance with an intelligence priority list based on "essential elements of information "(EEI). Special Reaction Force SOP should require that this individual immediately debrief those listed above who would be able to provide information early on. Another immediate task should be to brief the Security and Reconnaissance Team on this mission and intelligence requirements prior to their employment.

Thorough analysis of intelligence information should be accomplished by the USACIDC and intelligence personnel assembled as augmented to the IEOC, however, because the Special Reaction Force (Provost Marshal) must pass upward to the IEOC an estimate of the situation and recommendations for the development of options for military solutions to a hostage-taking problem, the Forward Command Post intelligence NCO must be capable of limited analysis.

Below is a list of EEI for use by Special Reaction Forces during terrorist events:

- precise statement of terrorist demands
- number, condition, identity and exact location of hostages
- number, condition, and identity of terrorists, to include names of leader

- Identity characteristics of both terrorists and hostages (e.g., clothing, distinguishable physical features).

- Terrorist weapons, explosives, equipment.

- Routines, movement patterns, and/or fixed positions of terrorists.

- Terrorist behavior - characteristics.

- Physical characteristics of barricaded area (building, other).

- Favorable access routes to barricaded area as well as entries for assault breakthroughs or other type entries.

- Favorable terrorist escape routes.

While much of the above information may be unobtainable, attempts to collect all must be made. Even partial information will aid the decision making process. All information gained should be passed speedily through the Forward Command Post to the Installation Emergency Operations Center (IEOC).

Actors and agencies not organic to the reaction force structure but still appropriate to the intelligence gathering effort during events can be:

- FBI analysts.
- Special agents, CIDC
- Military Intelligence analysts/operations.
- Contracted operatives/informants.
- Local and state police.
- Host-country intelligence agents.

The type and degree of participation of these personnel or agencies will, of course, be dependent upon the nature of the terrorist situation, and the availability of such personnel or agencies. For example, indirect contact - telephone or other type wire communication - may be just as effective a means of delivering information to the IEOC as direct contact. To synthesize the input from these personnel or agencies, the IEOC would do well to incorporate an all-source intelligence mechanism so that information valuable to the Forward Command Post and negotiators will be more thoroughly analyzed.

The reconnaissance element of the Security and Reconnaissance Team should have the equipment and flexibility to observe the target area (building w/terrorists and hostages) from as close a vantage point as possible. Situation-dependent, it is advisable for these personnel to wear civilian clothing. Both polaroid and 35mm cameras w/telescopic lens' should be used by this element, in addition to high-powered telescopes for continued observation.

Future reactions to terror can only benefit from intelligence gathered during incidents. CID and military intelligence personnel should combine to form criminal information and intelligence debriefing teams and every legal method possible should be used to extract maximum information from released hostages, captured terrorists, and counter terror force participants. This information should be forwarded to a centralized data bank where the information can be collated and then analyzed and delivered to government agencies with need-to-know. Information obtained should also be part of "after-action" reports to be maintained at installations as well as forwarded to higher headquarters and other interested Army agencies.

In March, 1977, the nation's capital witnessed three simultaneously coordinated terrorist incidents. This precedent implies that one incident on a military installation perpetrated by a terrorist group could be followed by another on the same day or shortly thereafter, necessitating that within an installation, when terror occurs, security elsewhere should be strengthened, and that coupled with this auxiliary security effort, there be an intelligence gathering effort, however fruitless the beginnings of such may appear. In this effort (criminal information and intelligence collection) CID, MI personnel, FBI and local police can be of much value. OCONUS, CIA and Host-country organizations may also be able to provide assistance. This assumes that a centralized intelligence gathering effort during terrorist events exist not only at installations but at the highest levels of government as well.

Negotiating. SAI has evaluated several negotiating organizational and tactical concepts and techniques ranging from participation of trained law enforcement personnel to area or public officials, to behavioral psychologists or psychiatrists, to deliberate use of females; to the direct approach, and to soft, or subtle behavior manipulation. Test results, however, have not shown conclusively that any organizational or tactical approach will in all cases serve better than another, or that a desired approach can always be implemented. In many cases, terrorists have determined their own negotiator, and often their behavior, or behavior performance (acting out) has caused negotiating tactics to shift to different modes. It appears, then, flexibility in the selection of negotiators and negotiating tactics should exist at installation levels. Negotiators should be capable of employing different negotiating techniques and have flexibility to switch from one to the other, that is, to be direct at one point, subtle, or indirect, at another.

This is not to suggest that there have resulted from analyses of negotating methods only play-it-by-ear responses. In fact, several analytical results have provided guidelines applicable to any hostage-taking situation. These are:

- Negotiators should not be authorized to make decisions on terrorist demands but rather communicate decisions
- Negotiators must develop trust, credibility and rapport with terrorists. This can be accomplished during negotiations by providing certain items that can benefit the terrorists without jeopardizing hostages, counter terror forces, or a U.S. government policy position.

- Selection of negotiating tactics should be based on learned characteristics of the terrorists. Quickly, negotiators must create a typology-profile of the terrorists, or terrorist leader with whom negotiations take place, in order to determine methods of approach. If a terrorist leader appears highly emotional, frightened and erratic, the negotiator will know to test his approaches gingerly and attempt behavior manipulation indirectly rather than directly.

Negotiators can be trained law enforcement personnel, not necessarily psychologists or psychiatrists. However, there are certain traits negotiators should have. These are:

- Ability to accept tension between two or more points of view, maintain perspective and continue to possess integrity of his or her own thoughts.
- Moral courage and integrity.
- Ability to role-play.
- Persuasiveness.
- Ability to demonstrate empathy without becoming emotionally entangled.
- Ability to foresee a negotiating approach in terms of a logical sequence of events and outcomes, yet an ability to cope with the unexpected by thinking and acting quickly and rationally.
- Patience.
- Quality of "listening" i.e., ability to serve as a sounding-board.
- Knowledge of human behavior, especially "aggressiveness".

- General knowledge of the political and other motivations of existing terrorist organizations.
- Ability to think as a terrorist and predict terrorist responses to his or her tactical approaches.

Many of the above traits can be cultivated in training and awareness programs and re-iterated in SOP of Special Reaction Forces. Still, because of the nature, or sensitivity, of the negotiations, and the enormous impact of negotiation ineffectiveness, it is recommended that assignments of negotiators be approved by installation commanders to insure that most of the above traits exist to a substantial degree within the selectee. Whether the selectee should be a trained military psychologist, a member of the CID, or a member of the Office of the Provost Marshal, should be decided at the installation where a more personal appraisal of selectees can be made. Negotiators can be individuals who have primary TOE-assigned duties, becoming negotiators as need arises. It is suggested they be selected from among volunteers, and that a test mechanism to show that candidates meet evaluative criteria to be negotiators be administered. FBI and major metropolitan area (NYC) police agencies have such examinations on hand.

Because the nature of hostage-taking events is so unpredictable, it is advisable that several negotiators be assigned on installations to meet a variety of situations. For example, ethnic, racial and religious motives behind terror can be more effectively dealt with by negotiators who have orientations similar to those of the perpetrator.

An additional comment about negotiators is that during negotiations they are the forward effort of counter terror activities. In immediate and on-going confrontation with the terrorists, they must be trusted by the Special Reaction Force commander and the IEOC. There can be only one negotiator at any given time. Interference from above can ignite harm and disruption, resulting in setback or stalemate. To avoid temptation of interference, negotiators should communicate from a location close to "but away from" the Forward Command Post, and visits to that location from higher authorities should be at a minimum. Further, it should be made clear in IEOC and Forward Command Post SOP that their inherent duties do not include negotiating.

As to where negotiators should fit within the counter terror force structure, SAI staff has experimentally placed them in the Forward Support Element of the Special Reaction Force within which is constituted a Negotiating Team. This team tentatively includes a Chief Negotiator and Assistant Negotiator(s). The Chief Negotiator maintains verbal contact with the terrorists and is relieved of such by the others when rest is required.

Also, as the Chief Negotiator is dealing directly with the terrorists, the Assistant Negotiator should be developing questions, new directions in negotiating tactics, analyzing terrorist responses and communicating developments to the Forward Command Post.

Safety of Hostages. For counter terror forces, the ultimate concern during hostage-taking situations must be (1), the safe release of hostages, (2) protection of lives and well-being of all participants, (3) apprehension of hostage-takers and (4) the protection of property and equipment. Bound and limited by the need to mobilize a counter terror plan and the force to activate and conduct such, counter terror forces can only proceed to care for hostages incrementally. These efforts should begin with attainment of information about the hostages and end with their safe release. Below is a tentative list of requirements:

- Determine number, condition and identity of hostages.
- Ascertain basic and other hostage needs (rations, clothing, etc) and attempt to arrange their delivery, via negotiations.

- Attempt, if necessary, to provide medical care and/or peaceful evacuation for wounded or ill hostages.

- Determine psychological state of hostages and attempt, via negotiations, to communicate directly to them to reduce their anxiety.

- Ascertain if any transference between terrorists and hostages has taken place and attempt to exploit this transference, via negotiations.

- Identify locations/positions of hostages in the barricaded area.

- Debrief any early-released hostages.

- Maintain, on site, medical and medical evacuation personnel/equipment.

- Continue to include the safety of hostages as the primary factor in plans for negotiations and other tactical efforts.

Hostages themselves can increase their own chances of survival by keeping in mind the following guidelines for hostage behavior:

- Try to stay as calm as possible. Be assured police and your family are doing all they can to see that you are safely released.

- Don't try to fight the terrorists should they push you around. Remember they are probably as afraid as you are and therefore unpredictable. They may also have prearranged plans to bring harm elsewhere should any of them be hurt by their hostages.

- Don't discuss personal matters. There is no reason to tell them anything about your family, job or property.

- Try to remember everything: what the terrorists say, what they look like, how they move This information could be valuable to the police later.
- Do what the terrorists tell you to do and don't dispute their commands.
- Attempt to escape only if it appears you will be successful and only when you are assured there will be no harm to other hostages. Never forget that your personal actions will have an effect on other hostages.
- Remember that hostage situations have rarely lasted more than two days. You will probably be fed and the percentage is high that you will be released.
- If you have an illness and require special medicines, let your captors know this.
- Try to calm other hostages who may be acting irrationally.
- Look and listen for opportunities to develop rapport with the terrorists.

Communications. Signal systems at the IEOC and Forward Command Post need be no different than those employed during other emergency operations. Communications security should, of course, be a primary consideration. On site, portable hand held radios should be provided leaders of all elements, to include components of the Special Reaction Team, and security and reconnaissance personnel. Command vehicles should maintain their vehicular radios, and telephones should be installed at the Forward Command Post, the location of the Negotiator, and the SRT's Assembly Area. The Negotiator, situation-dependent, may find it valuable to suggest to terrorists that a telephone be installed in the barricaded area if one does not exist. The loud-speaker system and the still picture cameras (Polaroid) authorized the Military Police Company by TOE should also be available for use.

Weapons and Equipment. SAI has evaluated current and projected technology as well as basic equipment to determine those items which would provide counter-terror advantages, especially for use by forward elements. Among type items in existing inventories are:

- M16 rifles
- Sniper-scopes
- Night Firing Devices (Starlite Scopes)
- 45-calibre automatic pistols
- 12-guage, 20" barrel, riot-type shotguns
- Water-cannons (Fire Dept.)
- Riot Control Agents
- Bayonets with scabbards
- Protective body-vests
- Protective head-gear
- CBR Detector Kits
- EOD bomb and explosive detection/disarmament kits
- Walkie-talkies (Motorola)
- TA312 telephones/field switchboard set
- Signal beepers, for tracking vehicles

- Binoculars
- Rapelling rope/scaling gear
- Light Assembly Kits
- Searchlights, vehicular-mounted
- Public Address Set
- Still camera (Polaroid)
- Medical aid/First-aid kits
- Automobile sedans
- Trucks, Utility
- Armored or protected (modified for protection) vehicle(s)
- ....In unique situations, helicopters.....

Except for five of the above items, all are authorized the Military Police Company, and except for Starlite Scopes all are readily available at most installations.

Liaison with Media and Public Officials. A terrorist act can grow into a media event. The platform that media can provide perpetrators is often the true objective of terrorist acts. Thus, the access that terrorists have to media can determine either a favorable or unfavorable outcome. If the terrorists demand media attention, such should be provided. It may be learned that media will serve as a catharsis for terrorist aggression, a hostility that, if not for access to media, could be directed toward hostages. Media, therefore, should be viewed by the counter terror force as a constructive adjunct to its counter terror plan. On the other hand, distorted perceptions of the objectives and immediate intentions of both terrorists and counter terrorists "on the part of media" could have disastrous results. An imperative, then, is that close liaison and rapport between the counter terror force and media should be accomplished immediately and sustained, and this should be the responsibility of the installation's Public Affairs Officer (PAO). The

PAO should insure that media personnel receive a true, up-to-date account of the terrorist event via methods that will not interfere with on-going operations, and that their presence, on site, be effectively coordinated. The installation PAO must also coordinate all military news releases through appropriate higher PAO channels to ensure uniform reporting procedures. Further, information that could be misconstrued by terrorists listening to/observing media, and produce dangerous overtones, should be withheld. Timely, well prepared briefings and accompaniment to on site activities can prevent negative media. Installation commanders should make the determination as to whether a media briefing location would be more effective close to the IEOC or by the Forward Command Post.

As to public officials, they too should be briefed accordingly and, unless required, they should not be allowed to attend on site activities. If required on site adequate protection should be provided.

Support (Logistics). In the tentative counter terror organizational MODEL, a Forward Support Element exists under control of the Forward Command Post and includes personnel to provide medical, transportation, rations, equipment and communications support. It is envisioned that much of what the Special Reaction Force needs for support is on hand on the installation and so the Forward Support Element includes but a small team (four personnel) to coordinate forward deliveries.

Special Reaction Force SOP should include methods and provisions for resupply, and any additional support beyond the SRF's capabilities should be requested from and coordinated by the IEOC.

Other Events

The hostage-taking event has received primary emphasis in this section. Although bombings and kidnappings have been acts directed against US Army personnel and property, there are no innovations or special strategies to meet these other events that have not been incorporated into existing security procedures of the US Army or of federal, state or local governments and which have not been treated in existing studies and documents. Therefore, the hostage-taking situation, so unique, complicated and potentially more dangerous than other events, as requested in the US Army RFP has received greater attention.

APPENDIX D

AWARENESS PROGRAM
EDUCATION - TRAINING

AWARENESS PROGRAM
EDUCATION - TRAINING

An overall program cf education and training to create awareness of terrorism must be implemented. Preconceived notions, varied perceptions, and common misunderstandings tend to create unnecessary and unproductive actions or expenditure of resources. This overall awareness program is two pronged with many facets. First, education of responsible individuals taking the form of formal instruction at branch centers and schools, orientations which could bring together military and civilian authorities in a controlled seminar forum, and articles in Army professional periodicals. Second, is the training of individuals and teams to attain skills and specialties to cope with terrorism. This combination of education and training can achieve a well balanced approach to countering terrorism - both before, during, and after the occurrence of such an act or incident.

EDUCATION PROGRAM

The Draft DOD Hardbook 2000.12, Subject: Protection of Department of Defense Personnel Abroad Against Terrorist Acts, contains a comprehensive bibliography outline on the subject of terrorism. This outline was examined in detail and it was determined that it is ideally suited to be the framework for developing and overall education program for the Army. This outline is particularly valuable in that the Draft DOD Handbook contains extensive reference lists for each of the subject areas listed below.

I. TERRORISM/COUNTER-TERRORISM - GENERAL

a. Definition

b. History

c. Theories & Concepts

d. Psychology

II. TERRORIST OPERATIONS

a. Urban Revolutionary Warfare

b. Terrorist Tactics

(1) General

(2) Kidnapping

(3) Assassination

(4) Bombing

(5) Skyjacking

(6) Others

c. Regional Activities

(1) Global

(2) North America

(3) South/Latin America

(4) Middle East

(5) Far East

(6) Europe

(7) USSR

(8) Africa

d. Terrorist Groups

(1) PFLP, Al-Fatah, Black September

(2) IRA

(3) Baader-Meinhof

(4) Others

e. Propaganda Activities

f. Incidents

g Material Resources

III. COUNTER-TERRORIST OPERATIONS

a. Policy/Jurisprudence Aspects

(1) U.S.

(2) International

b. Prevention Techniques

(1) General
(2) Individual
(3) Family/Residence
(4) Vehicle
(5) Facilities
(6) International

c. Repression Techniques

(1) General
(2) Kidnapping
(3) Assassination
(4) Bombing
(5) Skyjacking

d. Nuclear Related Activities

e. Media

Using the above outline varying programs were developed as follows (a detailed subject breakdown is shown at Figure D-1):

- Seminar for Senior Officers (16 hours) - These seminars are intended for grades O-6 and above. They are intended to provide a general background on the subject in order to deal more effectively in policy decisions, as well as crisis management.

- Seminar for Middle Management (32 hours) - These seminars are intended for grades O-3 to O-5. They are essentially patterned the same as seminars for senior officers, but in more detail. They are intended to provide a working knowledge of the terrorism problem.

- Program of Instruction for Army War College (24 hours) - This POI has its emphasis on terrorist operations, primarily in terrorist tactics and regional activities.

- Program of Instruction for Command and General Staff College (18 hours) - This POI emphasizes counter-terrorist operations, particularly prevention techniques.

- Program of Instruction for Officer Branch Basic Course (9 hrs) - This POI is intended to provide at all Branch Schools, an introduction to terrorism. Any more time devoted to the subject during the Officer basic course would tend to be counter productive during the formulation of basic Officer skills.

- Program of Instruction for Officer Branch Advanced Course (17 hours) - This POI is intended to provide, at all branch schools, a good understanding of terrorism and associated problems. It is structured the same as the basic course, but in more detail.

- Program of Instruction for Institute of Military Assistance (35 hours) - This POI stresses counter-terrorist operations, and particularly prevention techniques. IMA has been a primary activity in developing protective measures for individuals and has an existing training program; however, the recommended POI should be the minimum to be included in the various military assistance courses taught.

- Program of Instruction for Military Police School Special Course on Terrorism/Counter Terrorism (45 hours) - This is intended to be a special course conducted periodically by USAMPS. It should not be limited to Military Police officers and USACIDC personnel. It provides a good understanding and working knowledge for coping with terrorism.

- Program of Instruction for Military Intelligence (28 hours) - This POI is intended to provide Military Intelligence personnel a background in terrorist operations, regional activities, and an examination of specific terrorist groups. Additionally, background on counter terrorist operations is provided.

- Program of Instruction for Public Affairs Officers (15 hours) - This POI is intended to provide a broad, general background on all aspects of the terrorist problem. Particular emphasis is placed on U.S. and International policy aspects and the role of the media.

- Program of Instruction for Judge Advocates General (9 hours) - Ths POI provides an overview on terrorism merely to create a basic awareness of terrorism; however, emphasis is placed on jurisprudence aspects.

- Non-Resident Course by the Military Police School (45 hours) - The POI for this non-resident course is the same as the special resident course described above. Consideration should be given to establish a mobile training team capability to conduct this course.

- Orientation of Installation Commanders (16 hours) - This orientation is to be provided individuals selected to become installation commanders, either on an individual basis or in small groups. It is intended to provide the individual with a background on the terrorism problem and measures to cope with it.

- Orientation of Installation Provist Marshal Designees (24 hours) - This orientation provides the same background given the installation commander but most of the emphasis is placed on counter-terrorist operations. This is because the Provost Marshal will probably be responsible for the installation counter terrorism plan.

- Orientation of Key High Level Staff Officers (22 hours) - The candidates to receive this orientation should be selected on the basis of job responsibilities rather than grade. It is intended that a good background on the terorrism problem be provided those staff officers having responsibility for developing policies to counter terrorism and who could be involved in crisis management.

LINE NO.	
1	I. Terrorism/Counter-Terrorism - General
2	a. Definition
3	b. History
4	c. Therories and Concepts
5	d. Psychology
6	II. Terrorist Operations
7	a. Urban Revolutionary Warfare
8	b. Terrorist Tactics
9	(1) General
10	(2) Kidnapping
11	(3) Assassination
12	(4) Bombing
13	(5) Skyjacking
14	(6) Others
15	c. Regional Activities
16	(1) Global
17	(2) North America
18	(3) South/Latin America
19	(4) Middle East
20	(5) Far East
21	(6) Europe
22	(7) USSR
23	(8) Africa
24	d. Terrorist Groups
25	(1) PLO
26	(2) IRA
27	(3) Tupamaros
28	(4) Others
29	e. Propaganda Activities
30	f. Incidents
31	g. Material Resources

LINE NO.	
32	III. Counter-Terrorist Operations
33	a. Policy/Jurisprudence Aspects
34	(1) U.S.
35	(2) International
36	b. Prevention Techniques
37	(1) General
38	(2) Individual
39	(3) Family/Residence
40	(4) Vehicle
41	(5) Facilities
42	(6) International
43	c. Repression Techniques
44	(1) General
45	(2) Kidnapping
46	(3) Assassination
47	(4) Bombing
48	(5) Skyjacking
49	d. Nuclear Related Activities
50	e. Media

NOTES:

- Hours broken down to lettered subparagraphs only.
- Totals for major blocks of instruction are underlined, other numbers indicate subtotals.
- Further allocation of time on areas in numerical subparagraphs, i.e., (1), (2), etc., should be determined by the course planner.

KEY FOR LINE NUMBERS ON FIGURE D-1

	Seminar Sr. Military	Seminar Middle-Mgmt	POI Army War College	POI C & GSC	POI Off. Branch		POI IMA	POI MP School Special Course	POI MI	POI Public Affairs	POI JAG	Non-Resident MP School	Orientation Installation Commanders	Prov. Marshal Designees	Orientation Key High Level Staff
					Basic	Adv									
1	2	4	4	2	2	2	2	2	2	2	2	2	2	2	2
2	.5	1	1	.5	5	.5	.5	.5	.5	.5	.5	.5	.5	.5	.5
3	.5	1	1	.5	.5	.5	.5	.5	.5	.5	.5	.5	.5	.5	.5
4	.5	1	1	.5	.5	.5	.5	.5	.5	.5	.5	.5	.5	.5	.5
5	.5	1	1	.5	.5	.5	.5	.5	.5	.5	.5	.5	.5	.5	.5
6	6	12	12	6	2	4	8	18	16	7	2	18	6	6	12
7	1	1	2	1	1	1	1	1	2		1	1	1	1	2
8	2	3	2	2	1	1	2	4	3	2	1	4	1	1	2
9															
10															
11															
12															
13															
14															
15	.5	2	4	1			1	4	3	1		4	1	1	2
16															
17															
18															
19															
20															
21															
22															
23															
24	.5	2	2	.5		1	1	4	3			4	1	1	2
25															
26															
27															
28															
29	.5	1	.5	.5			1	1	1	2		1			
30	1	2	1	.5	1	1	1	2	2	2		2	1	1	2
31	.5	1	.5	.5			1	2	2			2	1	1	2
32	8	16	8	10	5	11	25	25	10	6	5	25	8	16	8
33	1	2	2	2	1	1	2	4	2	2	4	4	1	3	2
34															
35															
36	2	5	2	3	1	4	12	11	3			11	2	6	1
37															
38															
39															
40															
41															
42															
43	2	4	2	2	1	2	2	6	2			6	2	4	1
44															
45															
46															
47															
48															
49	1	2	1	1	1	2	1	2	2			2	1	1	2
50	2	3	1	2	1	2	2	2	1	4	1	2	2	2	2
	16	32	24	18	9	17	35	45	28	15	9	45	16	24	22

Figure D-1. Programs of Instruction

TRAINING PROGRAM

SAI has approached problems of counter terror training in sequential phases. In the initial phase, by first identifying operational events to be carried out by courter terror forces and individual members of these forces; second, by sorting out and differentiating operational units and individuals; third, by relating operational events to training subjects and those units and individuals required to conduct these events, thus, to be recipients of identifiable training subjects.

In the second phase, SAI investigated training methods in order to match and select options for the most practical way to deliver subjects to related recipients. The final phase consisted of development of a training MATRIX which includes and relates training subjects, recipients and methods. This MATRIX is presented on the following page. It is recommended that subjects be incorporated into a Program of Instruction (POI) that can be taught not only at the U.S. Army Military Police School but also at installations and sites. It is recommended further that those subjects designated for installations or sites in the form of CPX and field training exercises be repeated sufficiently to insure that newly-assigned personnel are aware of their requirements and proficiency in training is maintained.

Training Subjects	Training Mode	Students HP School	All, IEOC	Special Reaction Forces (Minus SRTs)	Special Reaction Teams (SRTs)
● Terrorism					
- Perpetiators	Lecture, Conference				
● Organizations		X	X	X	X
● Individuals		X	X	X	X
- Terrorist Goals & Objectives	Lecture, Conference				
● Political		X	X	X	X
● Religious/Ethnic. . . Separatist		X	X	X	X
● Mercenary		X	X	X	X
- Terrorist Acts & Methods of Operations	Lecture, Conference				
● Bombings		X	X	X	X
● Hostage-takings (barricades) and kidnappings		X	X	X	X
● Assassinations		X	X	X	X
● Hijacking/Skyjacking		X	X	X	X
● Other		X	X	X	X
- Terrorist Weapons and Technology	" and Demonstrations				
● Small arms		X	X	X	X
● Shoulder-fired hand-held missiles		X	X	X	X
● Bombing devices		X	X	X	X
● Counter-Terror	Lecture, Conference				
- Pre-event					
● Intelligence		X	X	X	X
● Security		X	X	X	X
- Crisis Management at Military Installations and Field Sites/Installation Emergency Operations Center (IEOC Operations)	Lecture, Conference, Practical Work, CPX's	X	X		
- Liaison w/Media and Public Officials	"	X	X	X	
- Special Reaction Force	Lecture, Conference	X	X	X	
● Organization		X	X	X	X
● Command Post Activities		X	X	X	X
● Communications		X	X	X	X
- Intelligence Collection during Operations	Lecture, Conference, Practical Work, CPX's	X	X	X	X
- Negotiating Tactics	Lecture, Conference, Practical Work, FTX's	X		X	
- Assault Tactics	" " "	X			X

Figure D-2. Training Program Matrix

Training Subjects	Training Mode	Students MP School	All, IEOC	Special Reaction Force (Minus SRTs)	Special Reaction Teams (SRTs)
(Cont'd)					
- Use of Snipers	Lecture, Conference, Practical Work, FTX's	X		X	X
- Safety of Hostages	Lecture, Conference, Practical Work, FTX s	X		X	X
- Weapons and Technology	Lecture, Practical Work, Demonstrations	X			
● M16 rifle . . . 12-guage shotgun . . . 45-Calibre pistol					X
● Sniperscopes					
● Night Optical Devices					X
● Riot Control Agents					X
● CBN Det ctor Kits					X
● Walkie-Talkies/TA-312's					X
- Special Training					X
● Rapelling					X
● Wall Scaling					X
● First Aid				X	X
● Driv ng Techniques				X	X

Figure D-2. Training Program Matrix (Cont'd)

APPENDIX E

INSTALLATION VULNERABILITY DETERMINATION SYSTEM

INSTALLATION VULNERABILITY DETERMINATION SYSTEM

- INTRODUCTION

If one attempts to treat a military installation in a strict generic category, and design countermeasures accordingly, the result would be wasted resources in terms of money and personnel. It is obvious some installations are more vulnerable to terrorist activities than others. For the purpose of this study it is not practical, nor is there time or money, to survey and individually design countermeasures for each U.S. Army installation. Additionally, such individual surveys would be valid only at the time such a survey was conducted. Conditions change. Installation are opened and closed. What is needed is a measuring device which provides a continuous means for determining priorities or actions to be taken in order to reduce any installation's vulnerability to terrorist acts.

The purpose of this installation vulnerability determination system is to provide a comparative measuring device for the relative vulnerability of groups of installations to terrorist acts or incidents. It is intended to be used as a staff officer's analytical tool to establish priorities of actions, and allocations of resources, to reduce the vulnerability while at the same time conserve manpower and money. The more vulnerable installations should be directed to take certain actions, and be allocated resources as appropriate, to reduce vulnerability. It is not necessary, or practical, for all installations to be directed to take the same actions. This system has purposely been kept relatively simple, does not involve sophisticated calculations, or highly specialized personnel to use it.

To determine the vulnerability of any given installation, in the absence of a specific threat based on hard intelligence, ten major factors are considered. These are broken down into subfactors and degrees with a point value assigned. As introduction to the detailed breakdown of the quantitative value, the major factors to be considered are:

- Installation characteristics and sensitivity
- Law enforcement resources
- Distance from urban areas
- Size of installation
- Routes for access and egress
- Area social environment
- Proximity to borders
- Distance from other U.S. military installations
- Terrain
- Communications with next higher echelon

It is readily apparent that any individual factor should not be a determinent in isolation of the other nine. There are obvious relationships between the factors. The system works on a scale of 0-100, whereby the higher the value the higher the vulnerability. Again, this is a system that can be used in the absence of a specific threat based on hard intelligence (a condition that has proven to be unlikely). If a specific threat against a given target, or targets, were provided then specific countermeasures can be developed to meet that threat.

To establish the quantitative values for the major factors, two independent judgemental processes were used with a combining of these processes in order to provide a degree of confidence to the values used. First, the SAI study team, while developing the system, applied values based on its experience and judgement. Second, a group experiment was conducted. In selecting the group it was desired that the participants be in the military law enforcement field, have between 5 and 10 years service, and that they not have a current assignment to an installation. The officer's advance class, in an academic environment at the U.S. Army Military Police School, provided an ideal group. Out of 58 participants, 50 valid responses were used to analyze statistically. The group of 50 valid responses represented a total of 235 years of law enforcement experience. After analysis, the findings of the experiment were matched to the initial SAI values, and while no great disparities occurred, the SAI values were influenced and changed accordingly.

- FACTOR QUANTIFICATION

- Installation Characteristics and Sensitivity (Total 18). This particular factor considers the "attractiveness" of a given installation as a target for a terrorist act. There are four sub-factors. First, a sub-factor considers personnel as hostage candidates. General Officers and foreign personnel assigned to the installation are considered. Second, the sensitivity of the installation mission is considered. Nuclear and chemical storage sites, ASA, would receive maximum value. R&D and training would receive lesser values. Third, an open post is assessed the maximum for this subfactor and a closed post is assigned no points. Fourth, an installation that is considered, or contains, a symbol of national significance is assessed the total number of points, e.g., Arlington National Cemetary; Ft. Monroe, Ft. McNair, etc. The points in the four sub-factors are additive to provide the resultant for the major factor.

.. 6 pts (VIP (1 pt/star) and foreign personnel (3 pts)
.. 6 pts Mission sensitivity (e.g., ASA, nuclear, chemical, training)
.. 3 pts Open post (zero for closed post)
.. 3 pts Symbolic (e.g., shrine, historic, etc.)

- Law Enforcement Resources (Total 13). Three categories of law enforcement resources are considered; i.e., military, federal and local. In that the law enforcement resource is responsible for law and order it should be given a heavy weight when quantifying vulnerability. These also are the people who have as a mission assessing and compensating for physical security weaknesses. The military is given more point value because they are immediately available and under the direct control of the installation Commander. While this function is normally performed by Military Police (MOS 95B) other military personnel resources may be counted if they perform law enforcement or physical security as a primary duty. The FBI and local authorities are considered supplements to the military resources organic to the installation; therefore, are not weighted as heavy. In this particular factor the higher the resource the lower the vulnerability, thus the lower the quantitative value.

.. Military Police (on duty or available within 15 minutes)

9 points	0-50
7	50-100
4	100-150
2	150-200
0	200 plus

.. FBI (OCONUS installations use host nation equivalent)

2 points max (use 1 agent/30 min ratio = 0 and go to max of 2)

.. Local Civil Authorities

2 points max (use 4 personnel/30 min ratio = 0 and go to max of 2)

- Distance from Urban Population Centers (Total 12).

For the purpose of this system an urban population center is defined as an urban area that exceeds 100,000 population. Almost without exception, experts on terrorism state that heavily populated urban areas are conducive to providing advantages to the terrorist. Concealment of supplies and equipment is made easier. Safe houses are more readily available, there is more of a tendency for popular support, and there is more freedom of movement in the relatively obscurity among the masses. On the other hand, small population center, or low population density areas, strangers are noticed and local law enforcement personnel tend to be close to the day to day pulse of the inhabitants. For the above reasons, a relatively high point assessment is given this factor as follows:

.. 12 pts	0-60 miles
.. 10 pts	60-90 miles
.. 6 pts	40-120 miles
.. 2 pts	120 plus miles

• Size of Installation (Total 10). The size of an installation contributes to vulnerability. Two major considerations are the physical size in area and the population. It is obvious that the larger the area the more difficult the physical security. One needs only to compare a nuclear weapon storage depot with Ft. Bragg, N.C. to illustrate this point. The larger the installation population the larger the number of potential targets created due to increased requirements for arms, ammunition, banks, schools, clubs, etc. Also, with increased population the probability for infiltration and support within is increased. The overall factor is weighted relatively heavy with equal assessment value assigned to size and population.

.. Area

-- 1 pt	10-100 sq mi
-- 3 pt	100-200 sq mi
-- 5 pt	200 plus sq mi

.. Population (military + civilian + dependents)

-- 1 pt	50-500
-- 2 pt	500-2500
-- 3 pt	2500-5000
-- 5 pt	5000 plus

• Routes for Access and Egress (Total 10). There are three major means of approaching and leaving a military installation, i.e., aircraft, vehicle, and boat. In quantifying this factor the following judgemental guidelines are used. Because of the capability of a helicopter to land and take off practically anywhere, all military installations are considered equally vulnerable. Therefore, only airfields, military and civilian, are measured. Road networks for vehicles should be judged in terms of freeways, major highways and secondary roads. The number of such roads approaching the installation should also be judged. For water routes only major waterways or large bodies of water should be considered. All three factors must be weighted in terms of poor, average, and excellent and the assessed values are additive.

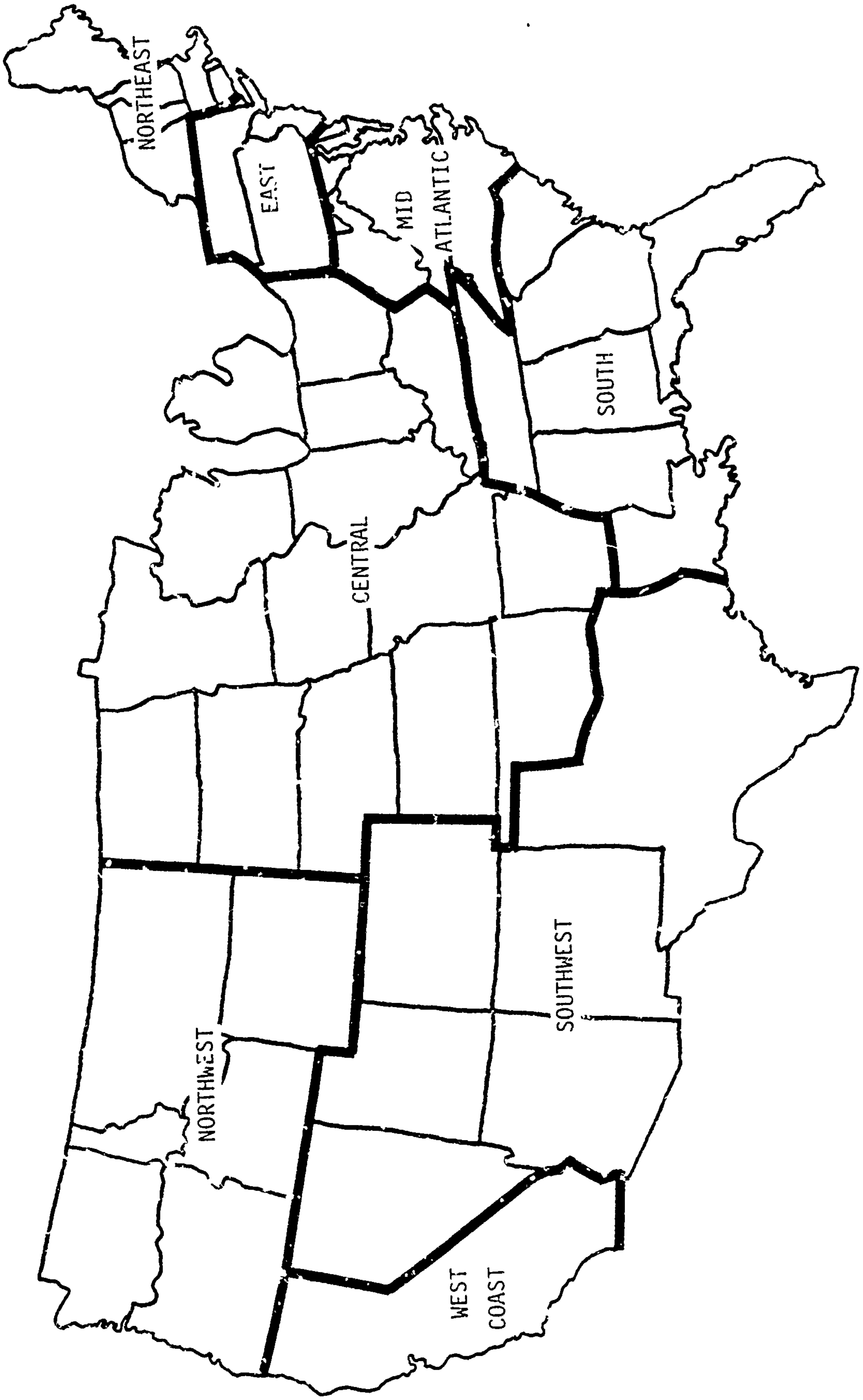
.. 1-4 pts	Airfields (poor-average-excellent)
.. 1-3 pts	Roads (poor-average-excellent)
.. 0-3 pts	Waterways (none-poor-average-excellent)

- Area Social Environment (Total 10). This factor is intended to give consideration to the social and ethnic environment, on a geographical basis, which is external to the installation. The vulnerability point assessments are based on the SAI threat analysis and other research papers. Some geographical areas of the U.S. either have a history of, or a tendency for, unrest and dissident elements within the society. For OCONUS installations the maximum value of 10 should be given. A map of the U.S. outlining the U.S. by the described geographical areas is shown at Figure 1.

.. 10 pts	West Coast
.. 5 pts	Southwest
.. 8 pts	East
.. 5 pts	Mid-Atlantic
.. 3 pts	South
.. 3 pts	Northeast
.. 3 pts	Central
.. 3 pts	Northwest

NOTE Some installations may be assessed a higher, or lower, value based on known local social or ethnic problems. All OCONUS installations receive a maximum assessment of 10.

- Proximity to Borders (Total 9). This factor of vulnerability takes into consideration the desirability of preparing for a terrorist attack in a foreign country and also escape after the act. The jurisdictional problems are readily apparent. The southern border of the


NORTHEAST
EAST
MID ATLANTIC
SOUTH
CENTRAL
SOUTHWEST
NORTHWEST
WEST COAST

U.S. is considered to pose a greater problem, in this respect, although this could change with time. In assessing values for OCONUS installations the maximum vulnerability value of 9 should be used. For CONUS installations only the closest border should be used.

.. Mexican Border

-- 9 pts	0-100 miles
-- 6 pts	100-500 miles
-- 2 pts	500 miles plus

.. Canadian Border

-- 6 pts	0-100 miles
-- 3 pts	100-500 miles
-- 1 pt	500 miles plus

NOTES: CONUS installations use closest border only
OCONUS installations assess maximum value of 9

- <u>Distance from Other U.S. Military Installations</u> (Total 8). This factor is considered because of mutual military support capability. Distance is used as the measurement which also is a major governing factor on response time. The other military installation in this case does not have to be U.S. Army since all U.S. military resources can be directed by the National Military Command Center or the Unified Command, as appropriate.

.. 0 pts	0-30 miles
.. 3 pts	30-60 miles
.. 6 pts	60-90 miles
.. 8 pts	90 miles plus

NOTE: If a local agreement for military support exists with a non-U.S. military installation, and the supporting force is exercised periodically, the non-U.S. installation may be quantified as above.

- Terrain (Total 5). Terrain adjacent to the installation is another external condition to be factored in the overall installation vulnerability. Some types of terrain or built up areas present certain advantages to planning and executing a successful terrorist act or incident. While relatively low in the overall quantitative value the type of terrain around an installation must not be completely discounted.

.. 5 pts	Built up area
.. 4 pts	Mountainous, forrested or conducive to concealment
.. 2 pts	Open

- Communications with Next Higher Echelon (Total 5). Communications with the next higher echelon by itself does not have a significant influence on determining the relative probability of a terrorist act occurring unless the perpetrators have knowledge of the effectiveness of the communications. Also, one should consider communications as having some influence on the outcome of certain terrorist acts. The more prolonged (e.g., hostage) the act the more influence communications can have in providing advice and assistance in coping with the situation. On the other hand, a bombing is a sudden event and the communications then serve primarily as a means of reporting. Both land line telephone and radio must be evaluated. Land line telephone is weighted higher than radio because it is more subject to interruption, either by terrorists or by accident. A dedicated communications system of either type has obvious advantages.

.. Land Line Telephone	
-- 4 pts	Non-Dedicated
-- 2 pts	Dedicated point-to-point
.. Radio	
-- 1 pt	Non-dedicated
-- 0 pts	Dedicated

- Bonus Points. There are two of the vulnerability factor quantifications that can be influenced resulting from actions taken by the installation commander. These two factors are Area Social Environment and Law Enforcement Resources.

The assessed vulnerability value of the Area Social Environment can be reduced to zero if the installation command and/or Provost Marshal is an active participant, on a regular basis, in meetings or councils with other area law enforcement agencies; e.g., local and state police, FBI, etc. With the restrictions imposed on Federal authorities in collection of domestic intelligence, close contact with state and local authorities provides the most effective means for staying current on the social environment surrounding the installation. With this type of current information specific measures may be developed to compensate for anticipated unusual events.

The assessed vulnerability value of the Law Enforcement factor can be reduced if the military law enforcement assets have certain capabilities. These can take the form of either unique equipment or training. Unique equipment such as V-100 type armored cars, military police aircraft, special firearms and suppression devices all tend to make law enforcement personnel more effective. Unique training such as sniper, special reaction team, negotiating gives additional capability to law enforcement personnel.

- Specific Targets

Due to the wide range of specific target candidates that may be possible no attempt is made to specify targets. AR 190-13, The Army Physical Security Program, provides excellent guidance in this regard, as well as a formal system for surveys and inspections. The following excerpts will confirm this finding.

- Para. 1-3g(b) Physical Security officers are responsible to the commander for identifying, in writing, activities specified by the commander as mission essential, as well as those particularly vulnerable to criminal acts or other distruptive activities.

- Para. 1-3g(c) Insuring that the activities above are inspected by physical security specialists to determine physical safeguards necessary to provide reasonable protection.

- Chapter 2. Physical Security Planning

Para. 2-1 Considerations in planning includes - armed security force, identifying specific targets.

-Para 2-1g Security plan will contain specific guidance on planning and action to be taken in response to demands, threats, or actions by terrorist groups.

- Chapter 3. Physical Security Inspections

These are annual inspections of mission essential/vulnerable areas and are an adjunct to the annual physical security survey.

Crime surveys are formal reviews and analysis of conditions within a facility/activity/area to detect crime, evaluate the opportunity to engage in criminal activity, and identify procedures conducive to criminal activity. They are not conducted on a recurring basis but rather are authorized by USACIDC commanders after determining the need.

- Chapter 4. Physical Security Surveys

These are an analysis of the efficiency and effectiveness of the physical security plan and are conducted annually. Copy of the survey forwarded to HQ DA who reviews and analyzes for overall Army security posture.

- Appendix - Examples of activities which may be considered mission essential/vulnerable areas.

COMMENT - Add key personnel, particularly general officers/commanders and schools/nurseries. Also things of high symbolic significance (Tomb of Unknown Soldier, Monuments, Statues, etc.)

It would be only natural to scrutinize the individual target potential at those installations rated high on the vulnerability scale. Likewise, the Physical Security Surveys for the more vulnerable installations should receive increased command attention.

APPENDIX F

THE INTELLIGENCE PROBLEM

COUNTERING TERRORISM ON MILITARY INSTALLATIONS
(The Intelligence Problem)

One universal constraint to planning effectiveness is the lack of intelligence. This constraint applies in varying degrees wherever US military installations may be. Insofar as is now known, no agency in the United States, local, state, or federal, to include the military, is authorized to collect domestic intelligence until a criminal act occurs or there is a clear threat to the national security within the context of current federal law. The root causes of this situation are theoretically the abuses of the system which resulted in the passage of the "Privacy Act" of December 31, 1974 and the issuance of Executive Order 11905 dated February 18, 1976, concerning United States Foreign Intelligence Activities.

Compounding the problem of obtaining information and intelligence posed by the aforementioned documents, is the succession of implementing instructions issued at every succeeding echelon down the line. Specifically these implementers consist of DOD directives (5200.27, 8 December 1975, Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense), Army Regulations (AR 380-13, 30 September 1974, Security, Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organizations), the Attorney General Guidelines (March 1976), Domestic Security Investigations), and a multitude of supplements and directives issued by commands and installations to "clarify and comply" with the source documents emanating from above.

As stated above, the basic reason for the flurry of restrictions being placed on intelligence gathering agencies was the abuse of some of the freedom given these agencies. However, if there have been abuses in the field of law enforcement intelligence, the sensible thing to do is to correct the abuses--and not to destroy our entire intelligence capability.[1]

Dr. William R. Kintner, President, Foreign Policy Research Institute, Inc., and former Ambassador to Thailand, addressed the Senate Subcommittee on Internal Security on 18 June 1976 and stated: "The first requirement of an effective anti-terrorist program is a comprehensive intelligence operation. Intelligence includes not only precise information but also an analytical capability which yields critical clues about the ideology, motivation, and likely action patterns of the terrorists and about the changing patterns of interlocks between the terrorist groups nationally and internationally. The possession of facts alone still does not solve the problem, but without the facts, the authorities are condemned to act in a blind and sometimes arbitrary or indiscriminate fashion, doing the terrorist's work for him. My first suggestion is, therefore, that the American people and their elected representatives must do some serious rethinking on this matter of law enforcement intelligence. Adequate intelligence is requirement number one in coping with the problem of terrorism--and in the absence of such intelligence the most dedicated police force in the world would not be able to effectively protect its community. Our society is bound to remain extremely vulnerable to terrorism so long as the present paralyzing restrictions on intelligence gathering capabilities persist. Furthermore, since terrorism frequently crosses natural frontiers, the intelligence capabilities of both the CIA and the FBI will have to be reinforced. I agree there is a need for guidelines. But the existence of guidelines does not require the kind of near total wipeout that now exists."[2] (Underlining added for emphasis.)

While Dr. Kintner was addressing his remarks primarily to the civilian community, it should be obvious even to the uninitiated that if the military is to combat terrorism, the same fundamental principles and requirements apply. Dr. Kintner went on to state that there is no substitute for public alertness in making it difficult for terrorists to function. This remark lends credence to the awareness program in the military that is advocated by SAI.

During the question and answer period following his prepared remarks at this same hearing, Dr. Kintner, in response to a question from Senator Scott, stated: "I think one thing your committee might well look into in the future is the nature of the guidelines which are being imposed on both the FBI and the metropolitan and State police forces with regard to this type of activity. For example, I have heard some police departments are restraining their people from even taking pictures of the demonstrators. I personally believe that this would be a deterrent. Demonstrators are very cool about police photographers. They like to see themselves on the "tube". They don't like to see themselves on the dossier."

Deputy Chief Robert L. Rabe of the District of Columbia Police Department stated at those same hearings, with Dr. Kintner, and again in an interview with SAI, in his office, that his current domestic intelligence is practically non-existant and that the D.C. Police intelligence unit had been disbanded on orders of the D.C. City Council.[3]

It has been the general consensus among military law enforcement officials interviewed by SAI that as a result of the restrictions placed on Federal (to include military) intelligence gathering agencies, their only source of information would be state and local officials. What is emerging is that in many of our major cities and states law enforcement intelligence files dealing with subversive and extremist organizations have been destroyed or otherwise made inaccesible, and that law enforcement officers now find themselves almost paralyzed by the pyramiding restrictions on intelligence operations. A few examples:[4]

- In New York State, law enforcement intelligence files painstakingly built up over a 30 year period have been locked up since September 1975 and most of the 24 members of the intelligence unit have been assigned to other duties.

During the question and answer period following his prepared remarks at this same hearing, Dr. Kintner, in response to a question from Senator Scott, stated: "I think one thing your committee might well look into in the future is the nature of the guidelines which are being imposed on both the FBI and the metropolitan and State police forces with regard to this type of activity. For example, I have heard some police departments are restraining their people from even taking pictures of the demonstrators. I personally believe that this would be a deterrent. Demonstrators are very cool about police photographers. They like to see themselves on the "tube". They don't like to see themselves on the dossier."

Deputy Chief Robert L. Rabe of the District of Columbia Police Department stated at those same hearings, with Dr. Kintner, and again in an interview with SAI, in his office, that his current domestic intelligence is practically non-existant and that the D.C. Police intelligence unit had been disbanded on orders of the D.C. City Council.[3]

It has been the general consensus among military law enforcement officials interviewed by SAI that as a result of the restrictions placed on Federal (to include military) intelligence gathering agencies, their only source of information would be state and local officials. What is emerging is that in many of our major cities and states law enforcement intelligence files dealing with subversive and extremist organizations have been destroyed or otherwise made inaccesible, and that law enforcement officers now find themselves almost paralyzed by the pyramiding restrictions on intelligence operations. A few examples:[4]

- In New York State, law enforcement intelligence files painstakingly built up over a 30 year period have been locked up since September 1975 and most of the 24 members of the intelligence unit have been assigned to other duties.

- In the state of Texas, as a result of a law suit, the Public Safety Division has destroyed over a million card entries--salvaging only those cards where convictions or indictments on criminal charges were involved. These were transferred to the criminal files.

- In New York City, almost 98 percent of approximately 1 million card entries were destroyed, leaving the intelligence unit with a reported 20,000 cards covering perhaps a third of this number of individuals.

- In Chicago, the files of the police intelligence unit have been impounded since March 1975 leaving the unit witout access to its own records.

- In Michigan, a Federal judge has ordered the State Police to destroy the files of their intelligence unit and disband the unit. This ruling is being contested.

- In Pittsburgh, the intelligence unit has been wiped out, and in other cities they have been reduced to levels which make it impossible for them to operate effectively.

- In Los Angeles, New York and other major cities, the controlling criterion governing law enforcement intelligence is that no entry may be made about any person simply on the basis of membership in the Communist Party or the Trotskyist or Maoist organizations, or even in violence-prone groups such as the [names deleted to comply with AR 380-13].

From the foregoing, it is apparent that an individual's record of conviction or indictment on a criminal charge facilitates an intelligence organization's retention of law enforcement information. Law enforcement and the criminal intelligence generated in support of its investigative functions is not predicated on convictions, indictments, or even arrests, but instead upon credible information indicating criminal activity. Consequently, law enforcement is not as hampered by restrictions as intelligence; however, intelligence access to law enforcement records is restricted and may result in false analysis and underestimation of the threat posed. The free exchange of information between intelligence and law enforcement organizations is necessary, if terrorism is to be successfully combatted. The synergy resulting from a joint threat assessment is essential and predicated on the belief that terrorism requires the best efforts of all, not the singularly directed efforts of law enforcement. To further reinforce this argument, is it any wonder that the Yugoslavian Ambassador denounced U.S. security precautions after his Embassy had been bombed for the third time on June 9, 1976. The State Department's "profound regrets" are no substitutes for sound intelligence procedures, which are the chief arm of domestic security.[5] Further, in October 1975, in hearings before the Senate Subcommittee on Internal Security, four of this country's top police experts on terrorist bombings all complained about the difficulties under which they were operating because of the destruction or inactivation of intelligence files and the increasing restrictions on their intelligence capabilities. Sergeant Arleigh McCree of the Los Angeles Police Department told the subcommittee that intelligence is relatively non-existant among our major police departments today.

Following the resolution of the recent wave of terror in Washington, D. C., T. R. Reid, a Washington Post staff writer, reported in the March 11, 1977 edition of the Post that some D. C. police officials and one member of Congress complained that restrictions on intelligence-gathering activities had hampered police in dealing with the recent terrorist actions in the Nation's capital. Further that officers said they had maintained extensive files until about 1974. They said the files were destroyed in the wake of sharp public criticism of police surveillance of political and racial groups. An official in the Metropolitan Police intelligence unit said the lack of intelligence had hindered police in their attempts to negotiate with the terrorist leaders. Rep Larry McDonald (D-GA) went further charging in a speech on the House floor that the successful seizure of three buildings was "a direct result of the lack of advance information" police could have obtained from ongoing surveillance.

Certainly the first move that the military should make is to address the tendency to provide for increased restrictions as each headquarters publishes implementers, or as the implementers are interpreted and enforced. A concerted effort by all concerned to do that which is possible within the Congressional/Presidential constraints would be a logical and necessary first step. In doing so, such items as the following could be avoided:

- Purging of all telephone numbers and names of Federal, state and local officials with official responsibilities related to the control of civil disturbances, from the pertinent military plans. (Expressly permitted in DOD Directive 5200.25 and AR 380-13.)

This incident occurred at Ft. Bragg, N.C., and was reportedly done on the recommendation of the Office of the Inspector General HQ Department of the Army.

- Removal from intelligence files of written material identifying dissident persons and groups not affiliated with the Department of Defense even though this material was published and available to the general public. (Expressly permitted in AR 380-13 so long as it is not inserted in name or subject files.)

This incident occurred at the Terrorist section of the Institute for Military Assistance at Ft. Bragg, N.C.

- During discussions with the intelligence community at HQ USAREUR it was stated that no serious direct threat against U.S. military installations existed and that for political reasons it would be more advantageous for the terrorist to attack West German targets.[6] Within two weeks after this discussion the Officer's Club at Rhein-Main AFB and the NCO Club at Bad Hersfeld were both destroyed by terrorists.

While it may be presumptuous to believe that intelligence was available that would indicate these incidents might occur, aggressive collection effort on the part of US agencies might have uncovered leads. This action falls within those actions permissible under Executive Order 11905 but according to interviews with agents at the operating level, their actions are being restrained by orders and policy from HQ USAREUR to the point that they feel completely impotent with respect to their intelligence gathering responsibilities.

Conclusion:

Arthur Fulton summarized the situation in his case study presented to the Senior Seminar in Foreign Policy, by stating:

"One point on which all authorities agree is the need for improved intelligence on terrorists of all philosophies. In the United States this is a sensitive matter at this time. The fallout from "Watergate." the repercussions of numerous inquiries into the activities of intelligence agencies, the increasing concern over privacy and the outrage over wire-tapping, all lead to a downgrading of intelligence capabilities rather than an improvement. The plea of Director Clarence M. Kelley of the FBI for legislation providing for controlled domestic wiretapping falls on deaf ears. Local police rush to destroy intelligence files and dismantle intelligence squads because of suits by civil action groups. It is hoped that we in the United States do not have to experience a ich" before we respond. You can be sure that if such a disaster occurs, the same critics now castigating and restraining intelligence agencies because of their past activities will be demanding explanations why those same intelligence agencies failed to know in advance of the coming crisis. The American people and their leaders must "bite the bullet" and, without further delay, arrive at a decision of just how much intelligence investigating they will permit and on whom the responsibility will lie if, in the future, it is not sufficient to cope with international or domestic terrorism."[7]

Recommendations:

1. The Service Secretaries and Commanders at all levels should institute a comprehensive review of all policies, directives, and regulations concerning responsibilities of--and restrictions placed upon--intelligence gathering agencies to remove "safe-siding" that inhibits exercise of full investigative/intelligence authority authorized by the Privacy Act and Executive Order 11905.

2. Commanders at all levels should require of their intelligence agencies the positive execution of intelligence activities authorized under the Privacy Act and the Executive Order, monitor compliance and punish individual abuses.

3. A comprehensive study should be accomplished which evaluates the present restrictions on intelligence gathering with the objective of submitting new legislation, if appropriate, permitting the gathering of intelligence sufficient to protect society while protecting individual rights.

FOOTNOTES

1. Senator Thurmond, Hearing before the Subcommittee to Investigate the Administration of the Internal Security Act and other Internal Security Laws, of the Committee on the Judiciary, United States Senate, Ninety-Fourth Congress, second session, 18 June 1976. Page 26.

2. Dr. William R. Kintner, Ibid, Page 28.

3. Deputy Chief Robert L. Rabe, Ibid, Page 43, and interview Washington, D C., 26 January 1977.

4. Dr. William R. Kintner, Ibid, Page 25.

5. Dr. William R. Kintner, Ibid, Page 25.

6. Interviews DCSI HQ USAREUR, November 1976.

7. "Countermeasures to Combat Terrorism at Major Events," Senior Seminar in Foreign Policy, 18th Session, Department of State, 1975-1976. Case Study by Arthur B. Fulton.

APPENDIX G

REVIEW OF REGULATIONS AND POLICY DOCUMENTS

APPENDIX G

REVIEW OF REGULATIONS AND PUBLICATIONS

During the course of the SAI study there were comprehensive reviews of regulations and publications, both in effect and in draft, promulgated at various levels of command. The two attachments provide comments on some of the most pertinent directives, particularly the Draft DoD Handbook 2000.12, Subject: Protection of Department of Defense Personnel Against Terrorist Acts. In addition, assistance was provided in developing Army Regulation 190-XX, Subject: Countering Terrorism and Other Major Disturbances on Military Installations. It is believed that this new regulation and an associated DA Pamphlet and/or Field Manual incorporating policies and procedures developed during this study should provide the Army with a strong program for countering terrorism, and other major disruptions, on its installations.

MEMORANDUM

22 April 1977

TO: LTC D. Gallagher
COTR Contract No. MDA903-76-C-0272
"Countering Terrorism on Military Installations"

FROM: Rowland B. Shriver, Jr. RBS
Principal Investigator

SUBJECT: Review of Draft DoD Manual 2000.12, Subj: Protection of Department of Defense Personnel Against Terrorist Acts

The subject manual has been reviewed. This review is intended to serve two purposes. First, to determine consistency with the findings of the SAI study team to date in order to prevent duplication of effort on the part of the contractor with what has already been accomplished by the DoD. Secondly, to assist in providing Army comments on the subject manual to OSD. Reviewing draft publications of this nature is considered to be within the terms of the current contract and not an additional item of work.

Overall, the draft manual provides good, detailed planning guidance for protection of personnel While the emphasis is on DoD personnel abroad, much of the guidance can, and should, be used by personnel in CONUS. The draft manual, understandably, contains numerous typographical errors. Since the review was made for overall content no attempt was made to provide editorial comments.

Due to certain portions of the manual being classified CONFIDENTIAL, the overall manual becomes CONFIDENTIAL. This tends to detract from the usefulness of the manual and would probably force users to extract and create supplements to avoid the handling of a classified document. The classified portions of the draft manual were scrutinized to determine what the overall effect would be should they not be included. As a result of this, it is concluded that the classified portions do not significantly add to the intended purpose of the manual and they should be deleted. A detailed review of the classified portions is attached. If it should be determined that the classified portions are necessary, an alternate solution is to have a classified supplement to the basic manual and derive separate distribution formulae for the basic manual and the supplement.

There is contradiction concerning the applicability of the draft manual. Paragraph 1-1 states, in part, "Information in this manual may be used as appropriate by DoD elements in the preparation of plans and programs dealing with any aspect of the terrorist threat". Paragraph 1-3 states, in part, "The objective of this manual is to provide guidance...." These statements lead one to believe that information in the manual is optional for use. However, paragraph 4-2 contains such words as "shall be reviewed and assessed in light of the provisions of this manual", "procedures guidance and instructions shall", "Chapters 6-9 of this manual....shall govern.....", and "....in accordance with the provisions of chapter 10 of this manual" - all tend to convey a mandatory meaning. Clarification is needed as to whether the manual is intended to be an optional planning guide or mandatory in nature.

Chapter 14 and Appendix H provide an excellent outline, along with an extensive bibliography, for establishing a program of education and awareness of the terrorist problem. SAI intends to use this outline as part of the development of an awareness program for the Army. This subject was included as part of the Second Quarterly Report, dated 15 March 1977.

The subject manual, if unclassified, is considered suitable for wide distribution throughout the Army. If distribution were made it would fill some of the informational gaps that were noted in SAI field visits. It could be the beginning of standardizing counter measures to terrorism on Army installations.

Attachment

REVIEW OF CLASSIFIED PORTIONS OF DRAFT DOD MANUAL 2000.12 DTD 1 MARCH 1977

Paragraph 3-3 - USG Organization, Policy and Procedures For Response to Incidents Abroad.

This paragraph deals primarily with the USG reaction to specific terrorist incidents abroad and the management structure. It also provides the USG policy on terrorist demands and negotiations. While the contents of this particular paragraph are of prime importance to high level decision makers it doesn't necessarily follow that it should be disseminated to the lowest echelon in the Army. Such a policy could be provided separately to selected decision makers within a crisis management structure.

Appendix A - Pattern of International Terrorism.

This appendix graphically displays statistics of international terrorist incidents 1970-1976. While nice to know, this information does not significantly add to the manual. It has been well established that terrorism has been a problem. Also, there appears to be a disparity between some of the tables. For example, the graph on page A-1 indicates an overall increase in terrorist incidents in 1976 over 1975; however, the tables on page A-3 indicate a declining trend. Statistics are interesting but are admittedly not very precise as regards terrorist incidents. The general treatment given this subject in paragraph 2-3, Development of Terrorism World-Wide, appears to be adequate for the intended purpose of this manual.

Appendix C - Potential Terrorist Weapons.

This appendix presents a vast amount of detailed technical information. There are so many technical details it is doubtful that the reader can comprehend, let alone even read, the contents. An alternative is to use the unclassified paragraphs in Sections II, III, IV, and V; which would provide a general description, concealability, and specific types for various categories of terrorist weapons. Detailed characteristics of these weapons could be made available through intelligence channels, on a need to know basis.

Appendix D - Terrorist Incidents Against DOD Personnel.

The information portrayed in this one page appendix provides a geographical breakdown of terrorist incidents against DOD or affiliated personnel and installations during the period 1970-1975. This background information is nice to know but not essential for the overall intended purpose of the manual.

Appendix F - State Airgram 775, 5 February 1975.

This appendix consists of a compilation of policy guidance for State Department use. While the information is important for inter-agency coordination it is of questionable importance below Departmental level. Additionally, many of the specific procedures outlined in this appendix are also stated, in an unclassified manner, throughout the various chapters of the manual. Lastly, it is questionable as to the propriety of reproducing State Department classified correspondence in a DOD publication.

Appendix G - State Cable 283548, 2 December 1975.

This appendix is a retransmission of a State Department cable concerning US policies during abductions of Americans. The same comments stated above for Appendix F generally apply to Appendix G.

PROBLEM AND DISCUSSION

1. There is no US Army regulation or directive dealing comprehensively with the problem of terrorism; rather, there are regulations or directives which deal with isolated or peripheral aspects of the problem. Matters that are treated are:

- Physical security of installations and equipment (AR 190-13) (AR 190-3)
- Civil disturbances (AR 500-50)
- Protection of officials (AR 190-10)
- Serious incident reports (AR 190-40)
- Criteria for protection of nuclear weapons and nuclear storage facilities (AR 50-5)
- Acquisition and storage of information (AR 380-13)
- AR 190-45, AR 195-2, AR 195-9, AR 145-16, AR 340-21
- Liaison with Federal agencies (Memorandum of Understanding)
- Support of private sector during hijackings/skyjackings of aircraft.

Terrorist operations are complex. Often, the victims of acts of terror are not related to the target, or target audience. Regulations and directives supporting effective counter-terror programs must provide guidance on a wide spectrum of terrorist activities. These are:

- Bombings
- Kidnappings
- Hostage-taking/barricades
- Hijackings/skyjackings
- Assaults and ambushes
- Incendiary/arson attacks
- Assassination/murder

- Riots
- Threats
- Blackmail.

While the above are also criminal acts and need not be connected purely to terrorists, when they are perpetrated by terrorists the effects of the acts reach beyond the effects of similar acts conducted by criminals. Terrorist effects have political and social ramifications which extend far beyond locations where terrorists acts take place. The reactions of military personnel against terrorists on military installations can have positive or negative consequences world-wide. Thus, it is necessary that US Army personnel have guidance that relates specifically to the effects of terrorism and how such effects need to treated. Matters of concern which are <u>not covered or not covered adequately</u> in current US Army regulations or directives are:

- Command relationships (who is in charge, when? during terrorist incidents)
- Clarification/distinction among incidents (which are terrorist, which are criminal?)
- Clarification regarding supervisory relationships between US Army and FBI
- Duties and responsibilities at major subordinate commands (installations and sites)
- What to do initially against specific terrorist acts... reactions to:
  - Domestic terrorists
  - International and transnational terrorists (especially during kidnapping and hostage-taking/barricades)
- Size and composition of counter-terror forces

- Communications during counter-terror operations
- Negotiating and bargaining with terrorists
- Liaison with host country officials
- Security of personnel during terrorist operations
- Developing speedy intelligence during operations
- Divisions of responsibility among installation commanders, provost-marshals, CID personnel, military police commanders, other personnel initially on-scene
- Liaison with private sector officials/communities
- Reactions to, and use of, on-scene media (journalists, television and radio)
- Duties and responsibilities of Army public affairs officers
- Assistance and protection of hostages and kidnap victims during operations
- Counter-terror tactics (assaults, break-ins, defense, use of snipers, use of EOD teams)
- Rules of engagement (when and when not to fire weapons)
- Identifying terrorists by type early-on during operations
- Organizing available combat-arms units
- Sealing off operational areas
- Protecting innocent bystanders
- Providing safe-withdrawal to terrorists when such has been granted through bargaining procedures
- Modifying terrorist behavior during incidents (preventing unnecessary harm to hostages or other victims)
- Medical support

- Specific pre-emptive actions when terror is imminent:
    - Protection of dependents
    - Protection of potential official material targets
    - Protection of potential official human targets
    - Implementation of pre-determined security alert levels
    - Identifying, approaching and detaining suspected terrorists
    - Preventing epidemics of fear among Military and other populations, preventing "over-reaction"
    - Use of weapons
    - Rules of search
- Handling mentally disturbed terrorists
- Reporting terrorist incidents, or threats, separately from other serious incidents
- Responsibilities for counter-terror training and guidance regarding training subjects.

RECOMMENDATION

2. Terrorism is a growing world problem. Since 1968, there have been more than 900 incidents perpetrated by more than 140 groups in 50 countries, wounding around 1,700 persons, killing more than 800. Among potential targets of terrorists, US Army installations rank high. Military installations and personnel symbolize, to terrorists, authorities against which terrorists have directed their long-range objectives. A comprehensive US Army directive defining actions that must be taken against terrorists at all levels, from Hqs, Department of Army, down to subordinate field action units would certainly serve as a more

effective regulating instrument than an array of directives dealing with components of the problem, which could lead to confusion and omissions in the field.

PPELIMINARY COMMENTS, SPECIFIC EXISTING DIRECTIVES AND REGULATIONS

a. AR-190-11, Physical Security of Weapons, Ammunition, Explosives.

Para 1-3b...no emphasis on performance criteria during selection of arms room personnel.

Para 1-41...no mention of acceptable temporary substitutes, or of appropriate actions when standards have not been met due to circumstances beyond the control of the responsible commander.

Para 1-4m...if practical options were stated, there would be no need for exceptions.

Para 1-5b...not specific as to just who should be delegated authority...security, as a responsibility, should be placed in the hands of those subordinate commanders with direct experience... paragraph should state lower "type" command, so as to prevent the inexperienced from receiving the security mission.

Para 1-5c...there are no comments as to what happens wnen approved waivers are forwarded to HQDA.

Ch 2, Para 2-1...this paragraph allows local commanders to determine priority given to arms storage development. The priority should be fixed at HQDA level, especially when US Army installations are potential terrorist targets.

Para 2-2(2)...does not state who will conduct weapons inventories, nor how completed inventories will be validated, nor how inventories should be programmed (uniformity, staggered, how?) nor how a program of inventories is to be monitored.

Para 2-2(c)...does not cite actions when high incident rates of threat occur.

Para 2-2d(2)...should specify type systems...para should not be writcen so as to allow the intrusion detection system to be a substitute for guard or duty personnel at any time.

Ch 3, Para 3-1...not specific enough in defining who will conduct inventories, how inventories will be validated and monitored.

Para 3-1g...high degree of vulnerability regarding munitions, NOT defined...directive to major Army commanders to publish guidance should include comments as to required context of such guidance.

b. AR 380-13, Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organizations.

The thrust of this regulation reduces the Army's ability to collect, store, collate and analyze information on suspected terrorists or terrorist organizations operating in the United States until operations are conducted on military installations, and then intelligence collection must be restricted to the act itself. This may be the US terrorist's strongest suit. Paragraph six (6) provides for exceptions to the rule, but is vague in defining the degree of demonstrable threat required before Army officials can request to conduct special investigations without active incidents as justifiable background. The term "characterizations", which may mean "profile" or "modus operandi" or something less, is not clear.

c. AR 190-31, Department of Army Crime Prevention Program.

This regulation does not isolate terrorism as a type crime, therefore does not include specific pre-emption or terror countermeasures. However, if terrorism were to be listed specifically as a crime the regulation's listed Crime Survey would be a valuable instrument on susceptible installations for before-the-fact intelligence scanning.

d. Memorandum of Understanding, US Army and US Coast Guard, Department of Transportation.

This memorandum does not cover situations involving US Army personnel at Coast Guard installations when terror is directed against them specifically.

e. Annex O, "Garden Plot", Army Civil Disturbances Plan C... and letter citing understandings between DoD and Federal agencies, Subj: Military Support in Combatting Terrorism, Department of Justice, 10 November 1972.

These documents state that the FBI is in charge of counter-terror operations on military installations in the United States. Neglected are those situations when FBI personnel are unable to be on scene fast enough to implement control. The documents do not consider the immediate responsibilities of installation commanders for the safety of US Army personnel and/or equipment, which can be achieved best and hurriedly by an installation commander with full charge to make appropriate decisions.

f. AR 190-3, Physical Standards for Storage of CB Agents and Munitions...being rescinded.

APPENDIX H

MISCELLANEOUS

PERCEIVING THE TERRORIST THREAT IN CONUS

CONSIDERATIONS

Premise

Terror as a force in America appears to be de-escalating. Two hypotheses for this are (1), the Vietnam conflict ended, defusing anti-war factions, and (2) there is, and always has been, a lack of valid revolutionary causes in America. However, in de-escalation, or silence, exists little proof of intent. Silence among US terrorist groups can be evidence of defeat, or of reversed coils capable of future acts. Dormant appearances, by themselves, are poor indicators, especially when suspected reasons for terrorist silence other than the above have some validity. In view of such reasons, it is possible US terrorists are re-organizing, re-evaluating, even plotting.

Factors

Cues for actions adopted by terrorists are delivered by environmental stress. That is, political, social or other people-effected events (national and/or local) impact on terrorist decisions to increase, decrease or sustain responses. It is from these events that reasons for silence among terrorists can be perceived. Discussed below, in an effort to stimulate thought, are factors which can be in the undercurrent that motivates US terrorists.

Political. Leftists, it is known, viewed Watergate and its undermining of the Administration as a sort of victory over the "right". To them it meant a warm and wide glaze of new liberalism might appear acceptable to the body politic. With that Administration gone, leftists would not want a re-curving "right", which could have occurred if terrorists, after Vietnam and Watergate, instituted terror acts. Terror, normally left-wing associated, would have resulted in certain repressions, a swing "right" politically. This implies that extreme left terrorists have been held in check, perhaps by less extreme leftists, that is, in abeyance until a change in political climate.

Terror, as an issue, would benefit an incumbent during Presidential elections. Terrorists, not wanting to influence these elections, would lie low. Thus, if US terrorists groups have some political savvy, or can be reached by less extreme leftists who feel they have a stake in elections, a valid reason for terrorist silence exists.

Social. In minds of extreme leftists, quantum progressions in federal dollars for social programs have not stripped the country of major ills. To a terrorist, if he/she is politically/socially oriented left, America has too many have-nots, and only violence can correct the imbalance. Although silent, terrorists of this genre, who were active prior to the end of Vietnam and Watergate, remain such. Recently, one of these groups published "Prairie Fire", a manifesto that preaches violence.

It is not social conditions as they really are that press terrorists into particular actions. Rather, it is the way in which terrorists perceive social conditions, and what these perceptions are, that cause actions. Conditions may improve, but hard-core terrorists will stay terrorists until the last issue is resolved to their satisfaction. For terrorists, there is an array of issues in any societal framework. Were it not for extreme repression, the Soviet Union would have its run of terror. In America, when race, employment or war are not issues, terrorists pick other causes.

In reality, America does not have just revolutionary causes, but to terrorists, through their distorted vision, there are causes. Certainly, within a population over two hundred million, terrorists find each other.

Method. The only base-line precedents US terrorists have to develop campaigns are foreign examples which effective in the mid-sixties became obsolescent in the seventies. Latin American models served US terrorists until it became apparent that perfected local countermeasures easily reduce their effects. Uruguay's Tupamaros (whose terror tactics are rooted in those developed by Israel's

Irgun) and Brazil's FLN (led by Carlos Marighella) were the models. Both advocated urban terror aimed at causing over-reaction/repression by legal governments; but legal governments, once burned, invoked controlled measures. In the US, democratic principles guaranteed controlled response, thus terror by US groups fashioned by the Latin American models hardly got off the ground. Marighella's "Mini-Manual of the Urban Guerrila" proved effective in terms of providing "how-to" advice for the conduct of type tactics but ineffective as a spur to continued terror. In other words, US terrorists are without "strategy"; they do not have a methodology by which to institute terror with some assurance of success.

Still, no evidence exists that US terrorists are not in search of dogma, no data citing that the current silence is not a transitional period during which terrorists are attempting to evolve precise strategies from which to act later on. The manifesto "Prairie Fire" could be a type foreword to such strategies.

Recruiting. No doubt, as the Vietnam issue subsided, quasi- and true terrorists drifted away from extreme groups to re-join society. Often, last year's radical becomes tomorrow's corporate attorney, businessman or salesman. The ranks of US terror thinned considerably. Today, if terrorist groups are just skeletal, to survive they must recruit. This is another characteristic of transitional periods of radical organizations: burrowing underground in order to re-build cells.

When Vietnam was an issue, the era itself climatized a population fringe that spawned pseudo as well as real terrorists. Today, in America, the zeal for radicalism is spent. Only the hardcore, the extremists steeped in dogma, would agree to terrorist associations. Recruitment, then, is probably slow, deliberate, painstaking.

This, certainly, would be an indication of prolonged silence... also an indication that should terrorist groups grow, fibres will be tougher.

Impl'cations

Today, known US terrorists are inactive; however, organizations orce active have not disbanded. Silence being no indication of intent, it is possible a transitional 'seeding' phase is their approved activity-mode and that several internal developments can reach a confluence from which re-newed terror will spring. In truth, no one is sure what US terrorists are up to. But if a valid picture is out of focus, is it not better to develop alternative projections?

On the surface, US terrorists are silent but possibly 'in transition," biding time to develop new strategies, recruit, train. Conversely, while there has been silence involving political terrorists, there has been a rash of "particularistic" or "ethnic" terror. For example, recent acts perpetrated by Cuban exile groups in Maimi, the Croations, and Puerto Rican nationalists. From this, we can state terror is a real present threat. We could also perceive a terror threat not in view of a continuum o' acts originating from a planned campaign, but as the possibility of a single act drawn from a plan ignited impulsively by even one or two neophyte terrorists. More than once, a single act of terror has proliferated a dozen more. One act against a US-based military installation could initiate these. And if that one act seems to destroy property valued high monetarily, let alone take lives, then certainly terror is, now, a threat, and preventive measures are needed.

Base-Line Statistics

While most terrorists incidents between 1968 and 1975 occurred outside the United States, there has been a steady increase in the number of American targets. If the American target is the trend, certainly there is the probability of specific targets being selected in the US. If terror is "theater", that is, a spectacular message designed to attract world attention and receive payment on demand, then the American target, in America, will soon be, for terrorists transnational by type, the brass ring. Below are some persuasive data covering period 1968-1975.

- of 375 terrorist bombings, 136 were US targets, 59 of which were in the US

- of 123 kidnappings, 59 were of US citizens (12 in 1974... 26 in 1975)

- of 137 hijackings, 21 were US oriented

- of the total 913 terrorists acts, 330 were US oriented.

A Problem

Minimum activity (near-silence) melts interest in terror as a critical threat. Belief-systems desire credible information. Without hard intelligence, pathways toward pre-emptors and countermeasures are rolled up and shelved. Fields of targets are laid bare; so when future terrorists strike, success probabilities are greater.

In view of considerations discussed herein, to determine a threat analysis of the slightest number of US terrorist acts should not evolve would be remiss, and at some later point fatal.

Presently, law prohibits US agencies from developing intelligence on organizations and individuals not associated with specific acts. There must be an obvious link to a terrorist act before agencies such as the FBI can utilize operatives to investigate organizations or individuals. This gap, or stop, leaves those concerned about probable terror with little more than assumptions. Nevertheless, assumptions, combined with past data, serve as precursors to probabilities. That is, it is worth pursuing a premise that silence among US terrorists is a product of transition and that terror will occur.

Conclusion

Lack of intelligence on US terrorists precludes knowledge of their near-term intent. Instead of capitulating to this lack SAI intends to create specific case-probabilities playing terrorists against US Army installations, using public data on pase events and OCONUS examples to define type minimum, moderate and worst-case situations, subsequently to develop appropriate policies, plans and countermeasures to deal with each.

SUMMARY OF VISITS

During October and November 1976 the SAI study team made visits to the following U.S. Army installations:

Fort McNair, Washington, D. C.
Seneca Army Depot, New York
Fort Rucker, Alabama
Fort McLellan, Alabama
Fort Bragg, North Carolina
USAREUR, Heidelberg, Miesau, Kriegsfeld and Frohn-Muhle

These visits proved to be invaluable in collecting information, personal views concerning counter-terrorism, and absorbing the nature of the problems faced by responsible individuals at installation level. This "grass roots" input is vital in the formulation of realistic policies, concepts, and methods to counter terrorism on military installations. A general observation concerning the visits is that the outstanding cooperation and interest displayed by those individuals contacted greatly enhanced this information collection effort. Another overall observation is that many excellent individual efforts are being made to cope with the problem but all seem to be looking for a total coordinated Army program. The following represents highlights of each visit and is presented merely for information. Specific details, or elaboration, may be obtained from SAI, if desired.

- Military District of Washington, Ft. McNair, 6-7 October 1976

  - The CG, MDW displayed keen interest in the study and stated his concerns on the lack of domestic intelligence and DA policy re: terrorism, the policy and planning is oriented toward the climate of the late 60's, and that the degree of protection provided VIP should not be determined by the person being protected. The Garden Plot plans were reviewed and these plans could provide a good point of departure for counter-terrorist planning. There were varying perceptions of the threat but everyone agreed that "the Army has not addressed the matter". It was believed that the person in charge for terrorist crisis management, and an alternate, should be designated in advance. There was strong feeling about the lack of armored vehicles, such as the V-100. The MDW personnel were not aware of any DA guidance on dealing with a hostage situation. It was indicated that there should be a policy on things not to do, as a minimum. MDW has an outstanding regulation on coping with bomb threats, a copy of which was provided SAI. The Provost Marshal stated that although the area surrounding Ft. McNair is one of the highest crime areas of Washington, the post is calm. He attributed this directly to the professional, soldierly MPs at the entrance gate who are highly visible and represent law, order, and authority.

- As an additional note contact was made with the Inter American Defense College at Ft. McNair concerning perceptions of the threat against the Latin American students. It was stated there were no extraordinary precautions taken and none contemplated unless directed to do so.

● Seneca Army Depot, Romulus, New York, 18-20 October 1976

- Seneca Army Depot was visited in order to gain first hand information relating to physical security of a large depot containing sensitive items. Key points that emerged were:

-- Aliens in sensitive positions. The depot had been assigned military police personnel who were aliens. Correspondence voicing concern was forwarded to DARCOM. who sent it to HQ DA for comment. It was returned giving no relief, solution, or apparent concern. A specific case is now pending (Appendix H-3) The concern is that the DOD civilian guard force that provides external security and control, must be U.S. citizens but military security and technical personnel, in sensitive positions, within the exclusion area, can be aliens with or without declaring intent to become U.S. citizens.

--Installation Access - The Depot Commander stated he could not deny access to the installation administrative area if an individual had a DOD ID card, even though it is a closed post.

-- Personnel - It was stated several times that the depot needed more security personnel. A "Fifth Platoon" concept had been developed which would permit more flexibility in rotation of duties, training, etc. There is some validity to this because additional requirements keep getting imposed (e.g., recovery mission, special reaction teams, etc.) with no additional personnel authorization. It has a definite morale implication. There did not seem to be a major problem in maintaining the authorized strength. (The Fifth Platoon concept requires an additional 55 MPs).

-- Training Area - There was no good training area available. Rifle ranges are at Camp Drum but Reserve Components have priority.

-- Helicopters - Depot personnel all thought that one or two UH-1 helicopters would greatly enhance the security posture, particularly recovery operations.

-- Attitude Toward Physical Security Duties - It was felt that physical security functions were downgraded with respect to the overall law enforcement mission. The views were that it started with recruiting policies that advertise patrol cars and apprehension or the general image of a policeman with no mention of physical security and guarding things, thereby misleading the enlisted. This was then compounded by incomplete basic training and schooling prior to a physical security assignment. There was a very favorable opinion on establishing a physical security career field and MOS (95E). Interviews indicated that there was definite interest in learning physical security both as an Army career as well as preparing for a rapidly expanding civilian trade.

-- Physical Security Training - What limited physical security training there was during AIT contained little or no mention of terrorism and how to deal with it. Discussions showed that there were diverse individual views on dealing with a hostage situation and techniques for negotiating. It was felt that the MP School should have integrated training for Special Reaction Teams (SRT). On their own initiative, depot security personnel had researched and obtained material from the Los Angeles Police Department, Nassau County Police, newspapers, periodicals, etc. to develop training for the SRT. No guidance on the hostage situation had been provided. AR 50-5, Nuclear Surety represented the only definitive guidance.

-- Equipment - TO&E and TA equipment included M79 Grenade Launchers, .45 Cal Pistols, M-16 Rifles. The security company had 8 V-100 armored cars but were experiencing a 70 percent deadline rate, due primarily to shortage of parts. The V-100s were rebuilds from Letterkenny Army Depot and were issued by DARCOM special authorization. The armament and radios were to be issued as separate equipment and difficulty was being experienced in obtaining those items. Unit personnel were interested in a newer version, the V-150 manufactured by Cadillac-Gage. They were interested in obtaining starlight scopes and other night vision devices. The starlight scopes were on the TO&E but not available for issue because DARCOM has lower priority than other major commands with operational units with a STRAF mission. The security company was not authorized some basic equipment such as compasses and had only 1 pair of binoculars of 6 authorized.

-- Intelligence - Discussion indicated a possible morale problem which could further [illegible]e the already relative ineffectiveness in collection of information. The primary factor was the impact of the Privacy Act (AR 380-13) along with reduction of personnel. The MI field officer had coverage of 3/4 the state of New York which included 1/4 the population. Four years ago the office was authorized 9 personnel and the current authorization is 1. When the 1 agent goes on leave or TDY (up to 3 months) there is no coverage. The assigned MI agent was highly experienced and motivated. On his own he attended monthly meetings in Buffalo, New York with representation by all regional law enforcement agencies (e.g., state and local police, FAA, Customs and Immigration, FBI, etc.). This was assessed as being extremely valuable; however the MI agent could not file, except mentally, any material. On three separate occasions it was stressed that dissemination of reports of terrorist incidents on other DOD installations would greatly enhance training, motivation, and planning. There was strong feeling in this regard. They felt that they were working in a vacuum without knowledge of actual incidents. They attempted to glean this information by word of mouth, newspapers, TV, etc.

-- Miscellaneous

● Individuals disqualified from the PRP were not reassigned in a timely manner. This could cause morale problems because replacements cannot be requisitioned until vacancies exist.

● The military security supervisors felt that the DOD civilian guards could be a problem in a crisis situation.

● It was suggested that MP units with a STRAF mission conduct part of their training at the depot and thereby would be available for augmentation. This would permit special training of personnel in the 285th MP Co.

● There was mention of a HQ DA message with SECRET classification, announcing new restrictions on use of riot control agents.

● Depot personnel felt that some of the AR 50-5 security requirements were overly restrictive and unsuitable for their type installation. They would like to see some flexibility in tailoring requirements to their needs.

This visit had two way dividends. Much information was collected for the study effort and the discussions stimulated new ideas and concepts among depot security personnel as well.

● Fort Rucker, Alabama, 27-29 October 1976

This installation was selected to be representative of a relatively isolated post with a specialized training mission. Significant observations were :

- There seemed to be a general feeling of low probability regarding the possibility of Ft. Rucker being targetted for terrorist acts or incidents. This could be attributed to a lack of awareness and understanding concerning today's terrorism coupled with the inability to collect and file domestic intelligence.

- Ft. Rucker has a rather elaborate EOC with unique capabilities. The EOC was under the charge of a GS-12, who had been in that position for approximately 9 years. The facility is able to control all cable TV on the installation with an override capability on the commercial broadcasts and can function as a small TV studio. Radio communications equipment provided the capability of netting with emergency vehicles, aircraft, and PM operations. The EOC was responsible for writing contingency plans. At the time of the visit a new plan dealing with a terrorist situation was being staffed. The EOC prepares a contingency plan reference chart which serves as a quick reference of actions to be taken in emergency situations, as well as identify resources that may be required. For each event identified there is a detailed written contingency plan. Some principles that had been established for emergency planning were:

-- Establish a command post in the vicinity of the event.

-- Establish dedicated communications between the command post and the EOC.

-- Designate on-scene commander.

-- Control movement of personnel at the scene.

- Physical Security MOS. There did not appear to be support for establishment of a Physical Security MOS (95E). The PM preferred consideration of an ASI to identify physical security proficiency. This could be due to the fact tnat the primary function of the PMO at Ft. Rucker is law enforcement with the majority of the physical security function contracted.

- Physical Security Contract. Security of the flight line and ammo storage was contracted to Transco. Inc., Cincinnati, Ohio. It provides for approximately 110 personnel, uniforms, weapons, related equipment, and vehicles. The installation provides radios, training ammunition, and POL. The contractor is responsible for proficiency and 40 hours of annual training. There is a no-strike clause in the contract. Twenty contractors responded to the RFP and 12 physically surveyed the area to be secured. The cost of the current contract is $813,753/annum.

- Intelligence Div. The Intelligence Division on the installation staff was headed by a civilian who had considerable tenure. The primary function appeared to be processing requests for security clearances. There was no perception of a terrorist threat to the installation. It was admitted that the installation was vulnerable but would not be a target that terrorists would choose. The Intell Division provided information concerning training of foreign students and stated there were no special precautions taken because of these foreign elements. The projected input for next year (CY 77) is approximately 800. The following countries have been represented in training at Ft. Rucker:

Morocco
Denmark
Guatemala
Mexico
Britain
Germany
Iran
Spain
Argentina
Venezuela
Saudi Arabia
Norway
Thailand
Bolivia
Australia
Panama
Ethiopia
Korea
Canada
Peru
Taiwan
Israel
Chile

- Military Intelligence. The 902d MP Gp Resident Field Office was manned by two agents, in 1974 there were 5, and had area coverage of the southern half of Mississippi and Alabama along with the northern part of Florida. The local FBI agent, was located in Dothan, Alabama approximately 25 miles away. The resident office did receive a weekly intelligence report through MI channels but was Europe oriented. The agents did believe that the local environment (small agrarian non transient) had a favorable effect from an intelligence viewpoint. Local authorities knew what was going on in their jurisdiction. AR 380-13, Privacy Act et al had a definite effect on the morale and efficiency of the intelligence operatives. The agents did receive information from state and local authorities but could not file it. They retained it mentally.

- Criminal Investigation - The CID had responsibility for protection of VIP; however, the requirements for this by Ft. Rucker were few. The CID office maintained close liaison with local police authorities. In preparation for 4th of July activities they held meetings with the local authorities in order to coordinate jurisdiction, if required. The crime rate at Ft. Rucker was relatively low.

- Ft. McClellan, Alabama, 1-3 November 1976

The first day was spent with the installation security and law enforcement personnel.

Ft. McClellan is a relatively small installation, open post, with training (MP School and WAC Center and school) the primary mission. The 548th Supply and Service Bn represents the only "troop unit". As of 31 January 1976 the post population was 6,481 military, 2,765 civilians, and 1,781 dependents. There was awareness of the terrorist problem and some contingency planning had been accomplished. The Provost Marshal reported directly to the Chief of Staff rather than being submerged within another staff directorate. The 111th MP Co. which serves as the installation law enforcement element, is under the operational control of the Provost Marshal and was authorized 4 officers and 102 enlisted with 6 officers and 89 enlisted assigned. The significant points of discussion were:

-Provost Marshal - The Provost Marshal did perceive terrorism as a threat to Ft. McClellan because it would be a low risk target. While the installation is an open post all but two entrances are blocked except during morning, noon, and evening rush hours. He discussed the limited number of law enforcement personnel (approx 100) and that although Ft. Benning would provide back up forces the response would be approximately 90 minutes under perfect conditions and that a more realistic time would approximate 3 to 4 hours. He sits on local law enforcement councils and stated that e stablishing rapport with local authorities is imperative. He lamented the fact that the Civil

- Military Intelligence. There was one special agent assigned to the resident office. He had been in that job for approximately two years. He did give information concerning the U.S. Army Intelligence Agency (USAINTA). Effective 1 October 1976 USAINTA assumed an Army-wide mission whereas prior to that it was limited to CONUS. Effective 1 January 1977 ASA and USAINTA are to combine with the Headquarters to remain at Ft. Meade Maryland.

- Emergency Operations Center - The EOC was in the Directorate of Plans, Training, and Security - Plans and Operations Div. It consisted of desks for various staff elements, some basic communications equipment and administrative supplies. The installation does have Chemical Accident Incident Control plans and appeared prepared to handle that contingency. The EOC was managed by a civilian GS-11 who had been in the job for 10 years. He felt there should be a requirement, and guidance, for establishing an installation crisis management center with authorization documents for equipment. Presently, equipment is scrounged and the facility capability is left to the initiative of the individual in charge.

The remainder of the time was spent with the Military Police School. Only a brief summary is provided at this time. Much of what was discussed were concepts, and combat developments. Detailed material is to be forwarded to SAI but at the time of the writing of this report the material had not been received.

One significant point that should be noted is the distribution and installation of J-SIIDS (Joint Security Interior Intrusion Detection System). Information provided by the Combat Development Directorate, indicated that while issues were being made installation was experiencing delays and is shown graphically on Figure H-1.

Disturbance Orientation Course, which brought military and civilian law enforcement people together, was going to be discontinued. He suggested that the MP School should develop seminars on terrorism for combined civilian and military participants. He had strong conviction that countering terrorism on military installations should be a law enforcement function with Provost Marshal responsibility. He became very interested in the SAI study and fully agreed that there is no guidance to installations on terrorism but felt that it would be a mistake to provide too much detailed guidance.

- Contingency Plans. The PMO had prepared numerous contingency plans primarily for MP use. Of interest to the current SAI study were plans for handling bomb threats, security of government officials, a military assistance plan which provided for the 548th S&S Bn to provide back up when MP resources were exhausted. There also was a plan for dealing with hostage situations and this plan emphasized that the safety and welfare of the hostage was the primary consideration. Also, the hostage plan identified potential victims, all of which were key individuals in post money handling facilities, and did not give consideration to all potential terrorist hostages; e.g., the Commanding General.

- Criminal Investigation. A highly experienced CID agent had been in his current assignment approximately 3 months. For the previous five years he had been a member of the Personal Security Detachment at SHAPE, providing personal security for the SACEUR. In discussing his experiences he stated that in NATO Europe the terrorist threat was a prime consideration in planning personal protection for VIP. He did not feel the Army had done enough to emphasize the awareness of the terrorist problem in CID operations stating there appeared to be no handle on the hostage problem or jurisdiction. The CID office worked closely with the Anniston police authorities and also the local FBI agent whose office was in Anniston. It was indicated that Ft. McClellan had a relatively low crime rate.

DISTRIBUTION & INSTALLATIONS

J-SIIDS

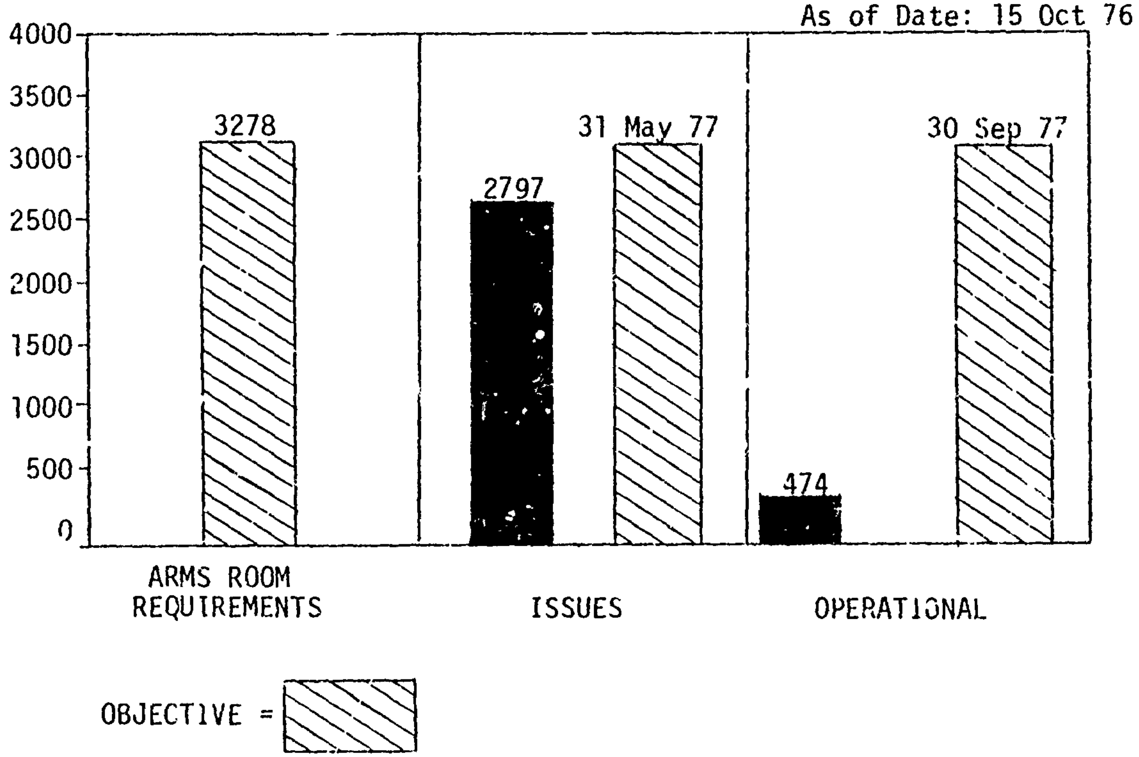


Figure H-1

- Ft. Bragg, North Carolina, 4-5 November 1976

The visit to this installation began with discussions at the Institute for Military Assistance (IMA). The purpose of these discussions was to determine what work had been accomplished on the subject of terrorism and what capability IMA had in this regard. Key points were:

- At the request of the Puerto Rico National Guard a 3 day seminar entitled, "Transnational Terrorism and Urban Violence" was prepared for 20 key command and staff officers of the PRNG. Upon completion of the seminar an after action report was prepared, a copy of which was provided to the SAI team. This after action report contained two significant recommendations -

(1) That IMA conduct a study to determine the feasibility of producing a senior level seminar based on the needs of the Army.

(2) That both IMA and the MP School participate in the development of the POI.

- The IMA, on its own initiative, has been very active in obtaining a vast amount of source material and information on the subject of terrorism from agencies outside of the government. It was stated there is "no DA source". By studying this source material, and by experience, a vast reservoir of expertise in terrorism exists at IMA.

- It was felt that one of the most practical approaches in deterring terrorist incidents would be to build images and create facades, while maintaining credibility. The same point had been brought up during previous visits. The IMA has devoted a portion of a manual on protection of MAAG and Missions against terrorism to this subject. A first step in this area is awareness of the problem by individuals charged with installation security.

- Just as its name implies, IMA is oriented toward MAAG and Missions. An integral part of this function is protection of personnel and facilities against terrorism. Much of this work could be translated to policy guidance for Army installations and personnel.

A day was spent visiting Ft. Bragg installation staff members and elements of XVIII Airborne Corps. The following observations were made:

- Ft. Bragg is an extremely large installation, open post, with a sizeable population. It would be practically impossible to secure the installation. Pope AFB is adjacent to the north boundary of the cantonement area and is in the process of becoming a closed post. There appeared to be wide variance in awareness of the terrorist problem.

- Military Police Aviation. As of 21 June 1975 the 16th MP Group had organic TO&E Military Police aviation assets. The aviation section was authorized 2 UH-1 utility helicopters and 3 OH-58 observation helicopters with 1 off and 4 wo pilots and 5 enlisted crew chiefs. The remaining enlisted personnel provided support functions for the section. The 16th MP Group had devised their own concept for utilization of MP aviation in the absence of any doctrine. The aircraft normally fly missions with a crew of 3 (pilot, crew chief, MP) and are able to communicate directly with MP patrol cars and also with MP operations. Spotlight systems for the OH-58 aircraft had been locally fabricated and the installed rotatable landing light on the UH-1's seemed to suffice. Nightly missions, at random times, were flown over sensitive areas, parking lots, and other areas conducive to crime. This technique apparently has proven successful in serving as a deterrent. There have been cases where the MP aircraft were used in pursuit situations. The roofs of MP patrol cars are numbered so the aircraft can provide direction to individual units. These MP aircraft are also used to support the Nuclear Accident/Incident Control Team, if required. At least one aircraft is on 1 hour reaction alert 24 hours/day. It was indicated that the 89th MP Group at Ft. Hood, TX was forming a similar MP aviation section. The 89th Gp had been in contact with the 16th MP Gp in order to obtain concepts for use and lessons learned. While the 16th MP Gp had done a commendable job in developing MP aviation concepts it would seem in-order for theMP School to use this operational experience, obtain from city and state law enforcement agencies police aviation concepts, and establish U.S. Army doctrine and policy.

- Armored Vehicles. At one time the installation law enforcement agency at Ft. Bragg was authorized M-113 APC's; however, they were replaced by V-100 Armored Cars. The V-100's are not used except for display purposes. They have been a maintenance headache. At the time of the visit 4 out of 6 authorized were deadlined due to lack of repair parts. This was indicated to be about normal. There had been no major problems with the armament systems (20 mm mini-guns and .50 cal mg). There had been major problems with the communications equipment. The V-100 Armored Cars and the ancillary equipment were on the installation TDA.

- Law Enforcement Resources. Due to the high troop population there was a relatively large amount of MP resources. There was the 503rd MP Bn with 3 line companies, the 118th MP Co (Abn) organic to HQ XVIII Abn Corps but under the operational control of the 16th MP Cp, the 58th MP Co., a part of the 16th MP Gp which ran the confinement facility and assumed the installation responsibility if the Corps deployed. The 82d Abn MP Co provided assistance in the installation law enforcement mission.

- G-2 and Military Intelligence. It was indicated that the best intelligence source was local and state police. They did provide intelligence but, for the most part, it could not be filed. The intelligence personnel stated that they "had to rely on institutional memory". The 902d MI Gp provided a daily operations report but apparently included only what was being reported within the Group. There was a definite feeling that some policies are overreaction to the Privacy Act. For example the names of civilian officials to be contacted in case of civil disturbances had to be deleted from plans and SOP. The MI agent further confirmed the decaying morale within the MI community due to the "hands tied" policies emanating from the Privacy Act.

- Criminal Investigation. It was stated that theft of arms and ammunition at Ft. Bragg was not a problem. There had been isolated cases but these had been cracked and there was no pattern or connection in these instances. The detachment commander suggested the possibility of MI supporting CID law enforcement in peacetime.

- Emergency Operations Center. The entire EOC orientation was geared to XVIII Abn Corps deployment and activities. There was little attention given to supporting a crisis on the installation. There was no apparent perception of a terrorist threat to the installation. For example, there was no contingency plan to provide assistance should the law enforcement resources be exhausted.

- U.S. Army, Europe, 15-19 October 1976

This visit was extremely valuable to the study effort in that many views were obtained, both individual and policy level, and provided an otherwise unobtainable comparison of awareness between CONUS installations/activities and that of individuals and activities in the environment of active terrorism. The USAREUR Provost Marshal Office had the trip extremely well planned which facilitated the maximum use of the limited time available. In general, there was universal interest in the SAI study and, an open and candid participation in discussions. While in many cases USAREUR faces unique problems in conflicting policy and guidance resulting from being a major Army Command, this did not appear to be the case in the subject of countering terrorism. This is because there is no specific guidance in this area and thus USAREUR has had latitude in dealing with terrorism. Key points which resulted from discussions were:

- General Blanchard, Commander-in-Chief. Approximately one hour and fifteen minutes were spent with the CinC in his office. GEN Blanchard was aware of the SAI visit and had requested this meeting. He was extremely interested and knowledgeable in the subject of terrorism. He had recently directed the Provost Marshal to prepare a paper on the subject and a command regulation. GEN Blanchard requested that he be provided a copy of the SAI Quarterly Management Report and any interim reports that may be published prior to the final report. It was also requested that USAREUR's Study Report be forwarded to SAI. GEN Blanchard discussed his philosophy of having plans to "accommodate varying conditions" analogous to DEFCONS and increased readiness. He thought this would conserve resources until indicators appeared which would precipitate positive actions. (The SAI study team has discussed this in general terms and this approach should be developed in some detail.)

While discussing VIP as prime hostage candidates he felt that he should have personal protection but it should be low key because of perceptions of the local populace. He also believed someone should define the level of VIP that required protection and what degree of protection should be provided. He did not appear to be opposed to the idea that the person being protected should not determine what protection should be provided, but that he should be consulted.

The SAI team related to GEN Blanchard the initial findings that the increasing restrictions on intelligence activities was creating both immediate and long term problems. He was keenly aware of the restrictions and was very interested in the comments concerning the decaying morale and initiative of the field operatives. When informed that SAI intended to track the originating Public Law and Executive Order through the implementing directives to determine if the original spirit and intent was over reacted to, he asked if anyone on the USAREUR staff had done the same thing upon publication of USAREUR guidance. He felt this was an excellent idea.

- LT GEN Cooper, Deputy Commander in Chief. GEN Cooper had requested this meeting after the visit of the SAI team had started. He was informed of the origin and status of the current study. While GEN Cooper is intimately involved in the security upgrade of nuclear sites he was keenly interested in the wider scope of the study. He felt that penetration of a nuclear site with the subsequent theft of a weapon was of paramount importance and concern. He agreed that much has been done and is planned to prevent such an occurrence.

- Office of the Provost Marshal. There was considerable discussion of the CinC directed study to the Provost Marshal on countering terrorism. A significant point is that while many principal staff agencies are involved the PMO, normally considered part of the special staff, had been given prime staff responsibility. Certain interim actions were being completed such as a message to the command on reporting procedures and actions to be taken within the headquarters and a message directing establishment of garrison security committees. This will be addressed below as they were DCSI proponency. The end product of this effort will be the publishing of USAREUR policy and guidance early in 1977.

Special weapons security and the current upgrade program was discussed in some detail. It is not appropriate to elaborate or comment on this program since it has high level interest and it receives intensive management. The USAREUR community structure was discussed in general terms and it was agreed that a visit to the Heidelberg Community Law Enforcement Agency would be of assistance and representative of the community concept. Mention was made of a EUCOM Special Reaction Team and a point of contact in ODCSOPS was given to discuss further details. When approached on the subject of physical security MOS for military policeman, the USAREUR Provost Marshal voiced definitive opposition to the concept. This further reinforces the opposition to this concept at the policy making level as compared to views expressed at the working level. The initial visit to the PMO provided an excellent introduction for the subsequent visits to USAREUR activities.

- ODCSOPS. A visit was made to the contingency plans branch to gain information on a EUCOM anti-terrorist force. The designation and location of this force is not included in this report due to the sensitivity of the information. A particular organization, which is under operational control of USCINCEUR, has a contingency mission of providing an anti-terrorist force with a capability of deploying on short notice within the EUCOM area of responsibility. It undergoes special training requirements and has special skills represented such as language, EOD, legal, psychological, sniper, and paramedic. Unique equipment is organic such as civilian type vans, special communications, high powered rifles, and the capability of operation in civilian clothes.

In a general discussion on terrorist special reaction teams it was indicated that Special Forces would lend themselves to this mission far more than rangers due to their organization being able to operate autonomously and the type of skills already represented. Additionally, the profile of a "Green Beret" represents maturity, extremely high motivation, a very positive attitude, ingrained with team operations, and is a volunteer who undergoes extremely rigorous training. When informed that the SAI study probably would pursue a special forces anti-terrorist reaction team concept, it was indicated that this would provide a valuable asset.

- DCSI. The USAREUR intelligence community has a distinct advantage over CONUS intelligence activities in that they can tap reliable sources of friendly foreign governments who do not have restrictions such as the Privacy Act and E.O. 11905. For example, the FRG has placed anti-terrorism at the national level with both intelligence and law enforcement disciplines. The BKA provides a daily intelligence summary cable to US intelligence agencies. The FRG is also capable of responding to terrorist acts or incidents from the national level. They have established anti-terrorist teams for almost immediate dispatch to trouble spots should the occasion arise. The FRG has enacted legislation to counter terrorism; for example, it is a federal crime to have knowledge of terrorist activities and not report this knowledge to proper authorities. This is an obvious assistance in collecting information. The MI has a liaison office with each German state which establishes a direct link to FRG intelligence sources. It is through this type of reliable input that DCSI is able to publish a weekly terrorist summary message, which receives wide distribution within the command. This type of information distribution has a positive effect of maintaining awareness to the terrorist threat. In addition, the 66th MI Group has prepared a new awareness briefing, complete with slides, to be used by the field operatives when giving orientations at the units they serve.

There was considerable discussion concerning a new letter of instruction further restricting US MI investigation and surveillance procedures. This is apparently the USAREUR implementation of E.O. 11905. Since this particular set of restrictions is an extremely sensitive issue there is a good possibility that each time instructions are promulgated they tend to be more restrictive than the intent of the original instruction. The end result on the operative is frustration, no initiative, and general lowering of morale. As a result, little useful intelligence is being generated with solely U.S. resources.

DCSI had taken two positive actions, which were included as part of the CinC directed study, which will assist in countering terrorism. One concerned procedures for reporting of terrorist information direct to the USAREUR Command Intelligence Support Indications Center (CISIC) which is physically located adjacent to the Operations Center. Intelligence analysts are on call in order to evaluate any information and provide feedback to the originator of the report and determine whether further actions within the command are necessary. The other action established garrison security committees within the CENTAG geographical area. Arrangements were made between USAREUR and the German Terrotorial Southern Command to establish regional, garrison level liaison among allied garrison commanders. It is envisioned that these garrison security committees will become the focal point of contacts to effect coordination of security matters of regional interest which will include but not be limited to mutual exchange of information on local security conditions, establishing local procedures for the provision of protective and security measures, and coordination of local actions to meet exigencies.

There was a discussion which touched on a variety of points. One concerned whether the subject of terrorism should be CI or MI. There did not seem to be any argument that countermeasures properly belonged to law enforcement. The MI "community" felt that MI was in the best position to verify the sources of terrorist information. It was believed that terrorists would require inside help to attack U.S. assets and it would not be politically wise to attack U.S. assets in the FRG. To date DCSI has had no experience o⁷ a valia advance warning of a terrorist act. They had issued warnings predicated on symbolic dates but had nc hard intelligen.e based on precise information. There was some apparent concern that the "terrorist threat" could get out of perspective and that awareness and understanding of the problem could go a long way in developing prudent countermeasures to terrorism.

- Office of the I ispector General. In discussions with the Technical Inspections Division, whose function is inspecting nuclear weapon activities, it was indicated that awareness of the terrorist threat is high at unit level. This is probably due, in part, to the high degree of command interest. During inspections situations are given to determine what degree of deadly force would be used in defeating a terrorist holding a hostage situation. While most responded according to existing policy there was some speculation as to consistency between a simulated versus actual situation.

- Office of the Political Advisor. The Political Adviso., was on leave and discussions were held with the Assistant POLAD. When asked questions concerning the status of forces agreement and jurisdic. onal matters it was indicated that these questions should be presented to the International Affairs Division of JAG. The Assistant POLAD aid provide information concerning the FRG action to divert some national border police assets to major airport security functions and to be more inclined to represent a less military organization appearance. (Note: While waiting for the return flight from Frankfurt airport, members of the border police were observed monitoring activities around the departure gates in uniform and carrying automatic weapons.)

- Office of the Judge Advocate. It was apparent that the International Affairs Division was extremely well qualified in International Law and the U.S. Status of Forces Agreement. When posed with a specific situation regarding jurisdiction (the CinC held hostage by terrorists in the barricaded command building) there was considerable discussion. Understandingly, they were cautious in responding to verbal hypothetical situations. The lawyers said that each case of jurisdiction would have to be judged on the specific situation at hand and that sometimes jurisdiction would be a matter of negotiation after the act had occurred. Also it was pointed out that certain legal opinions would be based on policy but that they were not aware of any policy re: the discussion at hand. It was agreed that it would be prudent to have certain legal guidelines prior to a terrorist act and that the same questions posed during the discussion would be valid questions to the General Counsel of both Department of Defense and State.

- Heidelberg Community. The Military Community has a Community Commander who is normally the senior military individual, much as the Post Commander in CONUS. There is also a Commander of the U.S. Military Community Activity whose role is similar to the Deputy Installation Commander in CONUS. In the case of Heidelberg the Provost Marshal/law enforcement element was designated the Directorate of Public Safety. All MP assets, to include the USAREUR Honor Guard, was under operational control of this directorate. He was also responsible for providing personal security for the CinC. It was stated that there was not very much guidance on carrying out these functions but that a lot was done locally. As an example, there was close daily contact with local German police officials, to include the BKA. He said the BKA designates potential terrorist victims, the CinC being so designated. As a result, the personal security for the CinC was supplemented to some degree by German authorities. The community Provost Marshal is an excellent example of an energetic, practical and knowledgeable individual who uses a great deal of initiative to accomplish the job at hand. He believed that USAMPS should have some type of orientation for installation Provost Marshal designees.

- Miesau Army Depot. This depot is one of the largest ammunition depots in USAREUR and has received more than its share of notoriety due to incidents such as thefts, security personnel problems, and leadership. Unfortunately, the new Army Chief of Staff was to visit the next day and many of the key personnel were involved in the preparations for his visit. There was, however, an opportunity for detailed discussions with the Depot Provost Marshal.

Miesau Army Depot has approximately 27 miles of fenceline encompassing about 2500 acres. It stores all types of ammunition and also some track vehicle equipment for REFORGER units. There are between 1000-1500 German civilian employees. The majority of married military personnel live on the German economy rather than government quarters at Kaiserslautern or Landstuhl. The depot administrative area is considered an open post but people are checked upon entry and spot vehicle searches are made at the gate. The U.S. has jurisdiction within the fence. The sensitive portion of the depot, which has its own system of barriers and controls, is guarded by the 164th MP Physical Security Company. In addition, overall depot security forces consist of 38 dogs and handlers, 2 explosive detection dogs, 48 military police, and the 4099th Labor Service Company consisting of 240 personnel with mixed nationality (most Polish). To supplement the depot security one infantry company, which rotates every two weeks, is used for patrolling at night.

The Depot Provost Marshal has extremely good perception for the security problems and aggressively seeks improvements. He was concerned about security personnel becoming apathetic. This is due, according to him, to the mundane type tasks to be performed and that the MP's were disillusioned when first assigned to security duties. He believed that this could be overcome to a large degree if the MP's were briefed and oriented prior to arrival at the depot. One problem he faces is that of untrained dog handlers. While losses of ammunition had been reported it was felt that inventories had not been accurate, originating from the mass influx created by FRELOC, and the shortages were considered to be on paper rather than thefts. Improved inventory procedures should alleviate this problem. The infantry company, which is rotated every two weeks, likes this temporary duty because it provides a break in routine and it is temporary. Two improvements in security have been accomplished. Improved locks and hasps have been instal.ed on conventional storage structures and, to provide for improved control of personnel, picture badges have been issued. Both MI and CI support was considered to be good. He works closely with the local polizei but primarily in the law enforcement function rather than local intelligence.

- Kriegsfeld Army Depot. This depot, which has a high security area, is secured by an MP Physical Security Company. The Depot Commander was an energetic, outgoing individual who was aware of the realities of security problems and his attitude was reflected throughout the depot organization. The MP company commander was the same type individual, making for an ideal team to enhance security. A significant point arose during the discussions - that being no exercises are considered practices to include road blocks established by local German authorities. Very close planning had been worked out with the local police, to include a point-to-point telephone line. The people in charge knew the security plans to the letter and provisions had been made, and tested, to provide alternatives which provided flexibility. Morale of the physical security personnel appeared to be good and local innovations were practiced in the way of sponsored recreational activities such as ski trips and tours. Again it was voiced, rather emphatically, that the 95B MP assigned to physical security duties should receive more orientation prior to arrival at the unit. It was indicated that approximately 2 months was spent in preparing an individual to become fully effective. The MI support was good and monthly briefings and updates were given to all personnel. The local MI agents again expressed frustration in carrying out their functions efficiently. They felt "handcuffed". In spite of some adversities, the security of this depot should be considered outstanding - primarily because of the responsible individuals rather than the "system". The depot commander also expressed concern that safety and security of new weapons (i.e., LAW) could cause them not to be in the hands of the troops when needed.

- A Btry, 2d Bn, 56th AD Artillery. Security of the sensitive area was provided by 16 95B MP's. There has been a recent increase to

38 MP's authorized plus an MP Lt. as physical security officer. This increase should provide for less time an individual will be on duty with an obvious increase in morale resulting. The unit commander indicated he would like to have dogs to supplement his security force, but had not taken into consideration the associated problems in maintaining the dogs.

MEMOPANDUM - ALIENS IN NUCLEAR DUTY POSITIONS

MEMORANDUM

DATE: 26 October 1976

TO: Major Gallagher (COTR Contract No. MDA903-76-C-0272)

FROM: Rowland B. Shriver, Jr., Principal Investigator RBS
Science Applications, Inc.

SUBJECT: Aliens in Nuclear Duty Positions

During the period 18-20 October 1976 R. Shriver and J. Evans (Science Applications, Inc.) visited an Army depot in connection with HQ DA Contract No. MDA903-76-C-0272, "Countering Terrorism on Military Installations." A condition surfaced which is considered to be sufficiently serious to warrant immediate reporting along with recommendations for corrective action. The following is submitted in accordance with the terms of the cited contract and constitutes a spot report:

A Mexican female alien subject enlisted in the Army to become a nuclear weapons maintenance technician (MOS 55G). She received her technical training at Redstone Arsenal, Alabama, qualified for the Personnel Reliability Program in a critical position, and was subsequently assigned to an Army depot. During an interview she voluntarily stated that due to her family's situation she did not intend to become a U.S. citizen and planned to return to Mexico upon completion of her enlistment obligation. The Depot Commander decided not to place her in a critical position as defined in DOD Directive 5210.41, "Security Criteria and Standards for Protecting Nuclear Weapons." Correspondence outlining this situation was forwarded to HQ, DARCOM on 28 July 1976. On or about 20 August 1976 HQ

DARCOM forwarded the case to HQ DA for resolution. Informal inquiry indicates that the correspondence is currently at ODCSPER with LTC Jonn Glenn as the action officer.

This case points out the present poli y legally allows aliens with unknown motives to infiltrate the Army, and other military services, gain sensitive information, knowledge, act as an insider, and return to the native country with no recourse, such as extradition. It is a DOD wide problem.

It is recommended that:

- This case be forwarded to the Assistant Secretary of Defense (Comptroller) voicing concern as stated above along with a recommendation that DOD Directive 5210.42, "Nuclear Weapon Personnel Reliability Program" include a requirement that an individual must be a U.S. citizen to qualify for entry into the Personnel Reliability Program.

- AR 50-5, "Nuclear Surety" be changed to include the requirement as stated above.

RESPONSES BY SENIOR ARMY LAW ENFORCEMENT OFFICIALS TO SURVEY QUESTIONNAIRE

RESPONSES BY SENIOR ARMY LAW ENFORCEMENT OFFICIALS
TO SURVEY QUESTIONNAIRE

What do you perceive to be the terrorist threat within your area of responsibility?

- The potential is there and probably so are they - but who they are - where they are and what their plans are - is a great unknown to me.

- Dissidents intending to disrupt and disgrace the military operations. This goal is limited to a specific area or operation.

- The threat could be from any group of malcontents with real or fancied complaints against personnel or facilities. The imminence of the threat is difficult to predict. Today I estimate the threat as relatively low.

- In the Panama Canal Zone there could be three threats. One could be "Zonians", a 2d or 3d generation born in the CZ. Second, the Panamanians. Third, a foreign power wishing to embarrass the U.S.

- I take exception to consistent over use of "buzz word - terrorism." From law enforcement point of view, it is the criminal acts (against persons or property) which are important - not the underlying motive. In a loose sense of the word the threat is from disgruntled groups claiming credit for bombings of federal facilities.

- The threat is high with government buildings and/or dignitaries as targets.

- Minimal - but distinctly possible since my installation is extremely large, is an open thoroughfare, and far from homogenous.

- The literature today tends to define the terrorists as those who commit crimes with political motivations. Your (SAI) definition includes psychos and criminals. According to your (SAI) definition, the siezure of a hostage (plain old kidnapping) is always possible. I don't like your (SAI) definition.

What sources of local intelligence concerning terrorism are available to you?

- Pretty scarce.

- Gossip, rumor, political and social organizations as well as MI operatives.

- Unit personnel and internal unit reports, MI reports and assessments, newspapers and other news media, reports from higher headquarters, rumors, anonymous tips, and overt acts by any terrorist type groups.

- Perhaps one of our better sources is our own liaison team who daily have contacts with the local authorities.

- MI, local offices of Federal Agencies especially FBI, local police. Although there are restrictions on collection and storage there is nothing to preclude obtaining verbal information by face-to-face liaison.

- All kinds, FBI, etc. - but how good their intelligence is, in this new controlled environment, I don't know!

- Military Intelligence, local CID, DIS, FBI, Drug Enforcement Administration, local police.

- I don't know - I'm in USAMPS.

- Local law enforcement agencies and field offices of Federal Agencies.

What do you consider to be the prime targets for terrorist acts on installations within your area of responsibility?

- Arms rooms perhaps to obtain capability to go on to bigger and better things. Computer systems also very vulnerable.

- Storage sites containing sensitive munitions and activities with sensitive missions. Students in training, arms rooms, water supply, communications facility.

- There was, several months ago, one incident in which an Army airfield was the target of a bombing. Other potential targets include arms rooms and ammo storage areas.

- Those facilities which could be put out of business without a substantial loss involving time or money to repair the facility for later use.

- Prime targets (based on actual incidents) which could have been perpetrated by "terrorists" -

  - Central arms/ammo storage facilities (but not unit arms rooms)
  - Central power and telecommunications facilities
  - Major Army medical center
  - Arson or bombing against troop billets
  - Money handling activities
  - Major outport for sealift of cargo
  - Presence of "controversial groups", e.g., Vietnamese relocation
  - Anytime VIP are present.

- Classified documents, various Headquarters of key activities (symbolic targets)

- VIP, arms and munitions, aircraft

- VIP visitors, public utilities, clubs

- Sensitive munitions and materiel, sources of money

- Arms rooms, finance offices, bank

If there have been terrorist threats, or acts, within your area of responsibility who conducted them, when, with what means, and where? What were the lessons learned?

- The bombing incident referred to (airfield) was carried out at night with no personnel injuries and very little property damage. The FBI investigated.

- None

- Not to my knowledge

- Explosives detonated in parking lots and other deserted areas which would impact on civilian/dependent fears. They occurred during evening hours and periods of limited visibility. Security personnel are <u>not</u> the answer - personal awareness would be the best deterrent.

- No actual acts specifically by "terrorists", but bomb threats and similar incidents found to have been perpetrated by youths and mentally disturbed individuals. These pointed out the need for:

  - Joint PM/CID Task Force with one "command and control center."

  - Task force to include medical/fire fighting/EOC plus emergency reaction force.

- Not against our military installations. We only have bomb threats - so far all idle.

- To my knowledge there have been none.

- Don't know of any.

- None.

<u>What policy guidance has been provided to counter terrorism?</u>

- FBI speakers

- DOD Directive that addresses responsibility and proponency for terrorism - belongs to FBI but the Army should be prepared to support.

- None

- Without referring to my PM SOP it is impossible to quote regulation numbers here at the conference.

- There is now an ever increasing amount of material flowing down from Dept. of Army and various professional organizations.

- Command correspondence, TM's, FBI presentations

- So far as I know, other than the study being prepared under DA auspices, which will ultimately lead to guidance, there is none at present.

- Rely mostly on AR 380-series, CIA, and FBI material.

- Primarily warning documents; i.e., better look at your nuclear sites, etc.

- Very little

- None

What changes or additions to policy guidance would facilitate planning to counter terrorism?

- Define parameters of terrorism in order to assign responsibility for neutralizing terrorist activities.

- Make someone responsible for program.

- Have a checklist, directive in nature, whereby personnel would not live in a vulnerable area, provide domocile to duty transportation, have films which would be part of mandatory welcome briefings. (Note: this response was overseas oriented).

- As revealed by the SAI team, to date, there is an immediate, urgent need to direct that all PM develop (update) their emergency plans/SOP. These SOP need not be entitled "Anti-Terrorist" but should cover reactions to threats against key facilities/personnel. These plans must be tested periodically. Ultimately there is a need for DA Directives and training material on the subject.

- Clearer lines of authority to respond, clearer guidance on responsibility and jurisdiction, provision of resources.

- I'm not sure

- The identification of responsibilities. Who does what? Who is in charge? Who runs the scene? Policy on these subjects should be issued.

- This should be a DOD task force project of the highest priority. Planning and equipping of an interbureau strike force, highly trained in counter-terrorism.

- None

Within your area of responsibility, how are "crisis management" teams organized? What disciplines are represented?

- No such teams have been organized.

- I am not aware of local program. There is a plan which provides guidance but it is not widely publicized. (Note: The respondent did not have operational responsibilities).

- What teams!?

- MAAG Security Team consisting of full time PMO, Embassy representative, signal, EOD, security officer from each service and major activity, intel agencies, and also the most important - the PAO.

- No teams now; however, they should include MP and CID, PAO, SJA, medical, firefighting, EOD, and Chaplain.

- We do not have as yet crisis management teams formed. However, we do have active alert plans which would marshal all available resources in a short period of time. There is also excellent tie-in with civil police resources.

- Organized to meet the known or perceived threat with composition as needed depending on hostage(s) or bargaining position. Tied together through EOC operations.

- At present time: law enforcement, legal, and command.

- I don't know - I'm in USAMPS.

- None.

Regarding jurisdiction, who is "in charge" during a terrorist crisis? (At the scene of the incident)

- Unknown, probably Commander/Provost Marshal

- Terrorist incidents are primarily felonies, CID should have major responsibility. PM is a manager, not an operator - should not control scene.

- We have not had any terrorist problems; however, if we did it will probably be the CID. They are the most experienced in this area.

- On a Federal installation, the Senior Commander.

- Post Commander.

- Commander, unless he has delegated authority to the PM.

- Considering that, in essence, so called "terrorist crises" are, in fact, the perpetration of crimes the only logical individual who can be "in charge" is the Provost Marshal or his designated representative. The PM is the senior law enforcement official at the installation.

- The MP's

- Good question!

- Should be designated by a plan.

- Any number of people depending upon the location and situation. It could be the unit or installation commander, Provost Marshal, or commander of the counter terrorist force.

During an act of terror what type of command, control, and communications procedures would be used?

- A Command Group should be at the scene with the most direct radio, wire, and visual communications.

- Depends on post - but MP's normally have good commo and would probably be used.

- Military Police and MP Emergency Operations Center.

- Suggest a mobile operations center in the vicinity of the incident using MP radio net initially under "command" of the PM. There should be provision for wire commo, if situation permits.

- Command Directives, guidance, delegation of authority. Operational control exercised by appropriate representatives. Commo is critical to control!

- Post Commander will have centralized control with advice from PM. MP commo will be used extensively.

- Most expeditious and most available.

- We would use the same system we use during any other crisis type incident.

- CID agent at scene should be in charge. PM should back him up with outer perimeter security, traffic control, ambulance support. Use CID and PM commo. PM makes his "SWAT" team available to respond to agent in charge.

During an act of terror what would be the response elements and tactics?

- Every PM should have a platoon with 3 or 4 squads trained similar to a "SWAT" team.

- The same as reacting to a bank robbery. SOP governing this area would be used.

- We have special MP sniper teams formed and trained by the FBI. Riot control agents are available and the control of them and their use is incorporated in alert plans. Reaction is contingent on development of alert plan. - - -

- There must be developed a syllabus for the training of an "Emergency Reaction Force", which would include various disciplines. "Tactics" envisioned are neither new not unique. Included would be commo, reaction to emergency plans, first aid, crowd control, riot control formations. These are tasks already performed - or supposed to be performed by MP.

- Military Police and EOD

- Unknown

- Reaction force must have the capability to completely and thoroughly overwhelm the terrorists if the need arises. The reaction force must deal from a position of strength, real and apparent.

During an act of terror what type of procedures would be used during negotiations with terrorists (who would negotiate with what type technique)?

- A messenger type individual or a person who has little or no authority to approve or comply with the terrorist demands. This will give the Commander an edge so that he can delay or drag out the negotiations and wear down the terrorist. Also, it will give the Commander increased reaction and planning time.

- Depends on locale but probably would be referred to FBI unless total military personnel involvement.

- The negotiator could be PM or his representative, Chaplain, SJA, medical personnel (possibly a psychologist) - but not CID or installation CDR/CG.

- Difficult question. It depends on the situation. Probably the best trained ones (MI or CID).

- It is envisioned that Military Police Investigators will be used. They are slated to receive training in this art.

- Only the Commander or his designated representative would negotiate.

- A senior CID special agent would probably negotiate. The technique would depend on who the terrorists are, what they want, etc. However, we would make it clear that the negotiator will not have any authority at all. He can not promise anything and he must have time to get any answer, giving us time to react to the situation.

- Train both selected CID and MPI personnel in negotiations.

- The Commander.

During an act of terror how would the public affairs aspect be handled?

- Have PM support by coordinating press point inside outer perimeter.

- Would be handled as any other incident.

- Releases would be cleared through the Commander via the EOC.

- Our PAO is tied in closely with DA Public Affairs. In significant incidents releases would come from that level.

- Credibility is vital to prevent and/or neutralize the terrorism threat and to maintain excellent rapport with the public to assist in maintaining public support against hostile actions.

- No comment. PAO possesses necessary expertise to determine.

- A most important member of the security team.

- Biggest problem is to find seating space for all the news media that would show up.

- Incidents should be played down so as to deter immitators, prevent the forming of large crowds of onlookers, but yet released information must be the truth and factual.

During an act of terror what special applications would be employed?

- Depending upon the situation and location any type of reaction force or combination could be employed.

- A makeshift organization would result from whoever is available.

- Riot control agents

- Snipers included as part of a special reaction team

- Organizations, special equipment, and special training should be available to counter "hard-core" terrorists as a contingency capability for protection of people, property, and maintenance of law and order.

- Use of and escalation of force would be used as needed but only after determination of what kind of negotiation would be conducted and what the counter offers are.

- MP "SWAT" teams should have marksmen, gas, armored vehicles, and other special equipment available.

<u>What additional equipment and technology would you like to have to cope with terrorism?</u>

- That normally used by emergency teams - helicopters, armored cars, weaponry, communications.

- Edgewood Arsenal has a new foam that could be excellent anti-intrusion material for sensitive areas. Should be examined and tested widely.

- I would like to see a centralized type unit that could support several Army facilities, that has been trained for this type of operation with a short notice reaction time.

- We only need to expand our training. Added resources can be gotten from the civil police who are well equipped. We could use an armored vehicle (V-100 type).

- No special equipment is needed. The key is ready availability of standard equipment/ammunition. These factors <u>must</u> be considered in emergency plans.

- Communications and personal protection devices other than rifles and pistols. Weapons are more dangerous than the terrorists if in the hands of the wrong people.

- A non-lethal immediate incapacitating capability.

- A quick acting, non-lethal, temporary incapacitant which is odorless, colorless, and tasteless which can be delivered discretely.

- The answer to this question should be based upon the study and after action analysis of terrorist incidents.

Additional Comments Provided:

- The anti-terrorist reaction could be structured in the following manner:

    - CG, General Staff and Special Staff would handle command decisions of magnitude, such as meeting money demands, etc. Special Staff could, upon request, furnish advice to the scene commander on technical areas.

    - CID to control the scene itself and conduct negotiations. Special Agents have much experience in dealing with people. They are also exposed to crisis situations on a daily basis making them ideal for functioning in a terrorist situation. They work closely with the Command, and control the scene and anyone on it. When uniformed Military Police are used they should operate under the control of the scene commander.

    - Military Police would be ready to provide support in different areas, such as traffic control, SWAT operations, etc.

- Definition of terrorism is vital to development of sound doctrine; approved and accepted by responsible activities. Give it a "continued" sense of urgency to develop current solutions to respond to and neutralize the threa. Update contingency plans and training of law enforcement resources and interested supportive activities. We need to support now the effort to react to the most serious current threat to the U.S. - terrorism that could escalate to guerrilla warfare within the U.S. We commend the efforts so far, particularly that of DAPE-HRE with Science Applications, Inc. Well done-keep up the good work in a serious problem area.

- The most important idea is to stop efforts to identify "terrorist activity" as unique. From police point of view "counter-terrorism" is part of crime prevention (measures taken to preclude incidents based on development of police information and threat assessment) and reaction to criminal incidents. By stressing "newness" or "uniqueness" of "terrorism" DA is, in my view, de-emphasizing obvious immediate needs for intelligence, threat assessments and emergency plans. It is possible that too many PM are "waiting for doctrine."

- I think this survey is much less meaningful than it would be if you would have allowed conferees to take it back to home station and research some of the material - which would provide more accurate responses. None of us came prepared for such a questionnaire; therefore, many responses are general in nature and less accurate than they would be otherwise.